Summerfields

PRIMARY SCHOOL

we think... we learn... we grow...

eSafety Policy

Reviewed: 25th January 2018

Next Review: 25th January 2019

Signed: Hillman

SUMMERFIELDS PRIMARY SCHOOL
E-SAFETY POLICY

RATIONALE:

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school E-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Head Teacher and governors to the Senior Leaders and Classroom Teachers, Support Staff, parents, members of the community and the pupils themselves.

However, the use of new technology can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

ROLES AND RESPONSIBILITIES

Head teacher and/or E-safety Co-ordinator:-

- leads the e-safety committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents

- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- provides training and advice for staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments (see appendix 1)
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meeting/committee of Governors

Teaching and Support Staff:-

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy/ Agreement (AUP) (Appendix 3)
- they report any suspected misuse or problem to the E-Safety Co-ordinator /Headteacher for investigation/action/sanction
- digital communications with students/pupils (email/Virtual Learning Environment (VLE)/voice) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- they monitor ICT activity in lessons, extracurricular and extended school activities
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.

Pupils:-

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems (Appendix 4)
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Education

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Pupils should be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Technical – Infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the SEGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- All users will be provided with a username and password by the ICT Co-ordinator who will keep an up to date record of users and their usernames.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by IIF/Lightspeed. Any filtering issues should be reported to IIF.
- Any filtering issues should be reported immediately to SEGfL.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and/or Head Teacher.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system.
- An agreed policy is in place (Appendix) regarding the use of removable media (eg memory sticks/CDs/DVDs) by users on school workstations/portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.

- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

Use of digital images – Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. However, Summerfields recognises the dangers attached to the use of personal devices in school, and has the following procedures in place:

- Pupils may bring mobile phones into school but these must be left at the office and collected at the end of the school day.
- Staff may use mobile phones in the staffroom but these must not be taken into the classrooms or any other area where children are working. We would prefer that phones are kept in staff lockers.
- Parents and visitors are advised that mobile phones may not be used in school.
- From time to time, individuals may wish to bring in hand held devices such as PDAs or tablets. School is not responsible for any damage caused to these devices.
- Staff are allowed to access personal emails at suitable times.
- Chat rooms/IM and social networking sites are blocked using the IIF filter system.
- Blogs for school use are permitted.

Unsuitable/inappropriate activities

The school believes that the activities referred to in the following section would **be** inappropriate in a school context and users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images
- Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist material in UK
- Pornography
- Promotion of any kind of discrimination
- Promotion of racial or religious hatred
- Threatening behaviour, including promotion of physical violence or mental harm
- Any other information which may be offensive to colleagues or breaches the integrity of the school or brings the school into disrepute.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

actions should be followed in line with the flow chart in the full version of this policy, in particular the sections on reporting the incident to the police and the preservation of evidence.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

Developing/Monitoring/Review of this Policy

This e-safety policy has been developed by the school E-Safety Coordinator and Head Teacher and will be monitored and reviewed on a regular basis (at least annually, but as issues arise). A fuller version containing reporting flowcharts and details of sanctions etc. is available from the E-Safety Coordinator.

Signed ________________________________ Date________________

Signed ________________________________ Date________________