The Southfield Trust
E-Safety & Acceptable Use Policy

Principles

This e-safety policy was written building on the East Sussex Guidelines and government guidance. It operates in conjunction with other policies of The Southfield Trust. These include Child Protection, Bullying, Freedom of Information, Information Security and Access and The Social Media Policy. It is also imbedded into the Trust schools' practice.

At both The South Downs School and The Lindfield School, the e-Safety Policy covers the safe use of Internet and other electronic communications technologies such as mobile phones and wireless connectivity. The policy highlights the need to teach pupils about the benefits and risks of using new technologies both in and away from school. It will also provide safeguards and rules to guide staff, pupils and visitors in their online experiences.

Effective Practice in E-Safety

E-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and pupils; (see also Social Media Policy)
- A comprehensive, agreed and implemented e-Safety Policy;
- Secure, filtered broadband from RM SafetyNet Plus
- A school network that complies with national standards and specifications

This E-Safety Policy is part of the Trust Schools' Development Plans and relates to other policies including those for ICT, Behaviour including bullying) and the Child Protection policy.

The schools have appointed their Designated Child Protection Officers as the e-Safety Coordinators for each site. The Heads of School and the Executive Head Teacher can be contacted regarding any e-safety incidents in the absence of the Child Protection Officer.

Teaching and Learning

Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The schools have 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.

How Internet use will enhance learning

- Internet access will be designed expressly for pupil use and will include filtering appropriate to the age and needs of the pupils.
- Should it be appropriate to the needs of individual pupils, they will be taught what Internet use is acceptable and what is not, and given clear objectives for Internet use.
- Pupils will be taught how to use the Internet according to the requirements of their individual learning programmes and their specific needs. This could include the use of the Internet in research.
- Pupils will be shown how to publish and present information to a wider audience should this be appropriate.

Managing Internet Access

Information system security

- The Schools ICT systems security will be reviewed regularly by Premier services.

- Virus protection will be updated regularly; it is now on automatic update by the Local Authority. However staff laptops should be brought into school on a regular basis to access this automatic update.

E-mail

Using e-mail may not be relevant to all pupils as part of their learning programmes.

- 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 as suspicious and attachments not opened unless the author is known.
- E-mail from pupils to external bodies must be agreed by a member of staff before being sent in order to ensure that it is appropriate.

Published content and the School's Learning Platform

- Staff or pupil personal contact information will not be published. The contact details given online should be for the school office.
- At both schools the content of both the web sites and VLPs is moderated by the Heads of School. Overall editorial responsibility also rests with them.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused.
- Full names of pupils will not be used anywhere on the Learning Platform or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Work can only be published with the permission of the pupil and parents/carers.

- Pupil image file names will not refer to the pupil by name.
- 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

- If used by individual pupils the school will control access to social networking sites. Such sites will be accessed only under supervision, and education in their safe use will be given.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- The Trust Social Media policy should be read in conjunction with this policy

Managing filtering

- Both The South Downs School and the Lindfield schools will work with the East Sussex, RM and Becta guidelines to ensure that systems to protect pupils are reviewed regularly and improved.
- If staff or pupils come across unsuitable on-line material, the site must be reported to an e-Safety Coordinator.

Managing video conferencing & webcam use

- At present video conferencing and webcam use is not used by the pupils at The Southfield Trust.

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.
- All staff are aware that technologies such as mobile phones with wireless Internet access and games machines including the Sony Play station, and Microsoft Xbox can bypass school filtering systems and present a new route to undesirable material and communications. Pupils are aware that this is not allowed on the school sites.

- The use by pupils of digital cameras or those in mobile phones is closely supervised and will be kept under review.
- The appropriate use of Learning Platforms will be discussed as the technology develops within the Trust.

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 Acceptable Use Agreement' before using any of the schools ICT resources. (see Appendix 3)
- For Key Stage 1 pupils, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Key Stage 2 pupils' access to the Internet will be closely monitored by class staff
- At Key Stages 3, 4 and 5, pupils' access to the Internet will be closely monitored by teaching staff in particular the ICT co-ordinator. Through the use of the installed software the teacher can monitor what is being looked at on each PC and turn off if needed. County filter websites or words on request in addition to the standard filtering system in place.

Assessing risks

- The schools 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 East Sussex can accept liability for any material accessed, or any consequences of Internet access.
- Premier (ESCC schools ICT service) 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 monitored by the e-safety coordinator.
- Any complaint about staff misuse must be referred to a Head of School or the Executive Headteacher.
- All e-safety incidents are recorded using the SIMS recording system.

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 where appropriate.
- E-Safety training will be embedded within the ICT scheme of work.
- The Trust has committed to delivering an annual e-safety awareness for staff and pupils at each school, managed by the ICT coordinators.

Staff and the e-Safety policy

- All staff will be directed to read the e-Safety Policy which will be available on the VLP and school web sites and its importance explained.
- 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 senior management 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 Schools e-Safety Policy in newsletters, the school brochure and on the Learning Platform.
- A list of e-safety resources for parents/carers will be maintained.

- All new parents will be asked to sign the parent /pupil agreement when their child starts school.
- The Trust schools send out guidance to parents on e-safety at home annually.

Appendix 1: Useful resources for teachers

BBC Stay Safe

www.bbc.co.uk/cbbc/help/safesurfing/

Becta

http://schools.becta.org.uk/index.php?section=is

Chat Danger

www.chatdanger.com/

Child Exploitation and Online Protection Centre

www.ceop.gov.uk/

Childnet

www.childnet-int.org/

Kidsmart

www.kidsmart.org.uk/

Think U Know

www.thinkuknow.co.uk/

Safer Children in the Digital World

www.dfes.gov.uk/byronreview/

Appendix 2: Useful resources for parents

Care for the family

www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf

Childnet International "Know It All" CD

http://publications.teachernet.gov.uk

Family Online Safe Institute

www.fosi.org

Internet Watch Foundation

www.iwf.org.uk

Parents Centre

www.parentscentre.gov.uk

Internet Safety Zone

www.Internetsafetyzone.com

The Byron Report

http://www.dcsf.gov.uk.byronreview/pdfs/Final%20Report%20Bookmarked.pdf

Becta e-safety quiz for parents

http://www.nextgenerationlearning.org.uk/en/benefits/E-Safety-Quiz/

Appendix 3: Staff Internet Use Statement

Misuse of School Computer Equipment

This statement has been drawn up in consultation with all the recognised Unions within the Education Department. Its purpose is to clarify the correct use of computer equipment by staff and the consequences of any misuse. This statement should be seen as a safeguard for staff and the employer. It applies to all staff working within the Education sector of the Local Authority, each of whom are required to sign it as an indication that they have read and understood it.

Computers (including laptops and other portable devices)

- Music files are not to be stored on school equipment or networks at any time.
- Storage of photographic files should be kept to a minimum.
- Personal documents relating to work should be stored under 'My Documents'. These files will be backed up by the ICT services regularly. The Local Authority reserves the right to access these drives.

Computer software

- It is not permitted to remove or copy computer software from the school premises for personal use.

Internet Usage

The Internet is an important research and information tool across the department and in schools and colleges The proper use of the Internet is encouraged. Accessing inappropriate material is likely to be viewed as a serious disciplinary offence up to dismissal. Inappropriate material should not knowingly be accessed on any school, college or Local Authority equipment whether it be in/outside work time or in/outside work premises. This includes portable equipment (i.e. lap-tops and iPads).

Inappropriate Materials

Inappropriate materials would cover any materials deemed unsuitable for staff to be accessing in relation to their post within a school / college or working for the Local Education Authority. Examples of such materials are pornographic sites, on-line gambling, extreme political sites, discriminatory sites of any sort (e.g. racist, sexist, ageist, homophobic, disablist. In fact all sites which conflict with the Council's equal opportunities policy) or sites which may produce a conflict of interest (e.g. signing petitions on line which are against school / Council policies/initiatives). This is a non-exhaustive list and should be used to guide staff when considering what sites to access.

It is recognised that staff may be able to access such sites by mistake when using search engines or when firewalls have not been able to prevent it. Where mistakes of this nature occur, staff must immediately notify the Executive Headteacher/Head of School/member of the senior management team / ICT co-ordinator in writing.

There may be occasions when staff are required to access sites that contain otherwise inappropriate materials in order to carry out their professional duties as determined by the curriculum (e.g. accessing tabloid newspapers and articles about terrorism with regard to a media studies course). Written permission should be sought from the Executive Headteacher/Head of School/member of the Senior Management Team to search for such sites and, having accessed the sites, a record given to him/her of the material and sites which have been used.

Executive Headteachers who access the Internet themselves, need to follow the same procedures outlined above, save that the Chair of Governors is to be consulted and informed.

Personal Use of the Internet

Personal use of school /college/department equipment and access to the Internet for personal use may be acceptable if used either before or after normal working hours or in line with school, college or department policy standards. Staff need to familiarise themselves with these standards. **The above guidance will still apply during time when the Internet is being accessed for personal use.**

Excessive personal use or personal use during working times may lead to disciplinary action.

Mobile Phones

The above guidance also applies to the use of mobile phones with Internet access. Staff should not keep mobile phones on their person during the school day. Phones should be kept in a pre-identified place in the classroom when staff are working with pupils. One exception to this is when a member of staff uses a personal mobile phone on an Educational visit. In such cases this person will be named on the Risk Assessment for the visit as the designated person.

Monitoring

All Internet use can be monitored including personal use.

The Southfield Trust Staff Internet Use Statement

I, ---------- confirm that I have read and understood the Southfield Trust Policy with regard to using the Internet on School equipment either in or out of the workplace/work time, and agree to abide by the terms and conditions of that statement. I am aware that the Local Education Authority's security software may record all Internet activity undertaken by me. I understand that any violation of the terms and conditions of this statement may lead to disciplinary action.

Signed ----------

Date ----------

School ----------

Please return this form to the Head of School.

A copy of this staff use of the Internet form should be in all Trust induction packs and a requirement for all new staff to sign.