

Lady Katherine Leveson
Church of England Primary School



E-Safety Policy

Responsibility of: KJ Brooks

Date: February 2010

Evaluation: February 2010

Reviewed: Annually in the Spring Term

Lady Katherine Leveson Church of England Primary School
Policy for E-safety

Overview:

This policy is written by K Brooks (ICT Co-ordinator and e-Safety Coordinator) , S Mitchell (PHSE) , A Byrne (Head teacher and Designated child protection co-ordinator).

This policy is built on the SMBC Schools e-Safety Policy and government guidance, and has been approved by governors after consultation with staff, parents and children

This policy is available to all staff; a copy is available on our network. It is available to parents in hard copy on request to the School Office, and is also on our website.

Purpose: We aim to enable a safe, responsible and mature approach to internet use, in order to raise standards and promote pupil achievement.

Rationale:

The Internet is an essential element in 21st century life for education, business and social interaction. It can support the professional work of staff and enhance the school's management functions. It facilitates the exchange of curriculum and administration data with SMBC and DfES;

Pupils' learning:

The school provides students with quality Internet access as part of their learning experience. They gain access to world wide resources, and take part in educational and cultural exchanges. The use of the extranet provides opportunities for home learning. Pupils use the Internet widely outside school, so E-safety is a vital part of pupils' education. They need to learn how to evaluate Internet information and to take care of their own safety and security.

Our school accesses the internet through Solgrid, which 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 are given clear objectives for Internet use, through the use of ThinkuKnow materials and the pupils' code of conduct. (See Appendix 1)

Staff role:

Staff guide pupils in on-line activities that support the learning outcomes planned for the pupils' age and maturity for example, by suggesting access to appropriate websites Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. They are encouraged to use internet information alongside books in our school library, and knowledge obtain on trips and visits. KS2 pupils have access to the school extranet (also through Solgrid)

Parental support:

Parents' attention is drawn to the School E-Safety Policy in newsletters, the school brochure and on the school Web site.

A partnership approach with parents is encouraged, through our website, newsletter and the use of parents' evenings with demonstrations and suggestions for safe home Internet use.

Key Principles

Internet Access

All school staff have access to the internet, which includes access to e-mail and extranet from home. All pupils can access the internet at school, although this is controlled by the teacher. (see Appendix 1) and at Key Stage 1, access to the Internet will be by directly supervised access to specific, approved on-line materials.

KS2 pupils, once they have received e-safety training in Yr 3, have access to the extranet from home.

The school has a current record of all staff and pupils who are granted Internet access.

All staff users must read sign and abide by the 'Acceptable ICT Use Policy' before using any school ICT resource. (Appendix 2)

Pupils agree to a Code of Conduct (Appendix 1), which part of the Home School Contract signed at the beginning of each year)

Evaluation and use of Internet content

The schools will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

If staff or pupils discover unsuitable sites, the URL (address), time, date and content is reported to Solihull ICT Services, and where appropriate, the school e-safety officer. Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Pupils are taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

The evaluation of on-line materials is a part of every subject.

School Website

Our website promotes our school and reflects its ethos. We keep it up to date. We seek written permission from parents before using pupils' pictures, names or work as part of our website. Photographs that include pupils are selected carefully and do not enable individual pupils to be clearly identified. Pupils' full names are not used anywhere on the Web site, particularly in association with photographs. Written permission from parents or carers is obtained before photographs of pupils are published on the school Web site. Images of staff are not published without consent.

Social networking sites

The school is sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offers appropriate advice through our website, Parents Evenings and pupil education in -safety.

Social networking sites and newsgroups are blocked unless a specific use is approved. Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc. Class and teacher blogs and wikis on the extranet site are pass word protected. Only KS2 pupils have access to the extranet and are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Children are encouraged to invite known friends only and deny access to others. They are advised not to publish specific and detailed private thoughts.

Staff should not communicate with pupils through social networking sites.

Pupils are encouraged to report anything that makes them feel uncomfortable and are aware of the concept of cyber-bullying (see Anti-Bullying policy)

E-mail

Staff are encouraged to use solgrid e-mail for all professional correspondence, and to keep their password secure. E-mail sent to external organisations is written carefully and authorised before sending, in the same way as a letter written on school headed paper. The forwarding of chain letters is not permitted.

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 without specific permission. Use of words included in the filtering/checking 'banned' list will be detected and logged

Access in school to external personal e-mail accounts may be blocked

Other Technologies

At present the school has no access to video conferencing.

The policy will be updated to cover use of other technology that may be used in the future.

Managing Information Services

The security of the school information systems is reviewed regularly. Our virus protection is updated regularly.

All portable data storage devices used in school are password protected and issued by school. Personal portable data storage devices are not used in school and therefore no images of children or children's data are kept by staff. Staff are allowed to take their school laptops home, and children's data is kept on these. They are password protected. School laptops are not left in cars.

Laptops should not be left unattended, but shut down or locked to protect sensitive material.

Data Protection

Personal data is recorded, processed, transferred and made available in compliance with to the Data Protection Act 1998.

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify an individual).

The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individuals rights
- Kept secure
- Transferred only to other countries with suitable security measures.

E-safety Complaints

E-safety complaints are dealt with using the normal complaints processes for the school.

Formal complaints of Internet misuse are dealt with by a senior member of staff

Any complaint about staff misuse must be referred to the head teacher who then uses the agreed SMBC procedures.

Monitoring and Evaluation

It is reviewed annually, or as technologies change.

Appendix 1

Internet Code of Conduct

I will

- keep my password secret.
- ask permission before using the internet.
- only use websites my teacher has chosen.
- use information appropriately.
- inform an adult if I find anything I do not like.
- only send e-mails to people my teacher has approved.
- send e-mails that are polite.
- never give out a home address or telephone number.
- never open e-mails from people I do not know.
- never arrange to meet anyone I do not know.



Appendix 2

Acceptable ICT Use Policy

At Lady Katherine Leveson School we use ICT to raise standards and promote pupil achievement. We aim to enable a safe, responsible and mature approach to internet use for both pupils and staff.

All staff and pupils have a username and password that gives access to both our network and Solgrid. Passwords must be secure, that is, they must not be shared or easily discovered. All personal data should be recorded, processed, transferred and made available in compliance with to the Data Protection Act 1998. For more detail refer to the e-safety policy.

All portable data storage devices used in school must be password protected and issued by school. Personal portable data storage devices are not used in school and therefore no images of children or children's data are kept by staff. Staff are allowed to take their school laptops home, and children's data is kept on these. They are password protected. School laptops must not be left in cars. Laptops should not be left unattended, but shut down or locked to protect sensitive material.

School photographs should only be stored on the school network. Check with school policies before publishing photographs, names or work. There is a list of pupils who have permissions.

Network

Users should respect the organisation of the network and file work as appropriate.

The work area (W: drive) and teachers' area (V: drive) are used by staff, details about the use of these drives (a 'Read me' document) is available within each area. Staff can access document and policies in the teachers' area. Staff should save work of a confidential nature in the appropriate area.

Be aware that pupils can access only the managed and resources areas.

Any practical problems should be brought to the attention of the Technician through the yellow book provided.

Staff should log off or lock a computer before leaving it unattended.

Internet use

All internet use is through Solgrid. All staff have access to Solgrid using their username and password.

Staff must use Solgrid e-mail for professional correspondence.

When working with pupils staff must check all material and websites are appropriate.

Any concerns about pupils' safety or inappropriate material should be brought to the attention of the Head teacher.

Staff are expected to check copyright.

All staff are advised to read copy of the school's e-safety policy, which is available, along with other policies, on the network in the teachers area.

Staff should not communicate with pupils through social networking sites.

Sign

Date