Acceptable and Responsible Internet Policy

Importance of the Internet in School:

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

2) How does the Internet benefit education?

- Access to world-wide educational resources.
- Inclusion in government initiatives such as the DfES ICT in Schools and the Virtual Teacher Centre (VTC) **http://vtc.ngfl.gov.uk**;
- Educational and cultural exchanges worldwide
- Cultural, vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for the whole school community
- Staff professional development through access to national developments, educational materials and good curriculum practice;
- Communication with support services, professional associations and colleagues;
- Improved access to technical support including remote management of networks;
- **E**xchange of curriculum and administration data with the LA and DfES
- Mentoring and peer support

3) How will Internet use enhance learning?

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

4) How will pupils learn to evaluate Internet content?

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT Co-ordinator. The service provided has a very strong firewall that filters all searches and certain sites are restricted totally.

Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

5) How should Web site content be managed?

- The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or pupils' home or personal information will not be published.
- Web site photographs that include pupils will be selected carefully and will be used in line with the school's photography policy.
- Pupils' full names will not be used anywhere on the Web site, 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.

· Senior leaders will take overall editorial responsibility and ensure that content is accurate and appropriate.

· The Web site should comply with the school's guidelines for publications.

· The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

· The school scans regularly their own web site to check links that have been made into their own sites and to remove links from potentially dangerous sources.

6) Can chat be made safe?

- Pupils will not be allowed access to public or unregulated chat rooms.
- Children should use only regulated educational chat environments. This use will be supervised and the importance of chat room safety emphasised.

7) How can emerging Internet applications be managed?

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

8) How will Internet access be authorised?

The school will keep a record of all staff who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave.

· All pupil access to the Internet will be by adult demonstration and supervision to specific, approved on-line materials.

· Parents will be informed that pupils will be provided with supervised Internet access (an example letter for schools is included as an appendix).

· Parents will be asked to sign and return a consent form. Please see the sample form later in this document.

9) How will the risks be assessed?

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.Methods to identify, assess and minimise risks will be reviewed regularly. The head teacher will ensure that the Internet policy is implemented and compliance with the policy monitored.

10) How will filtering be managed?

The technical strategies being developed to restrict access to inappropriate material fall into several overlapping types (commonly described as filtering):

Blocking strategies prevent access to a list of unsuitable sites or newsgroups. Maintenance of the blocking list is a major task as new sites appear every day.

A walled-garden or allow list provides access only to a list of approved sites. An allow list will inevitably restrict pupils' access to a narrow range of information.

Dynamic filtering examines the content of Web pages or e-mail for unsuitable words. Filtering of outgoing information such as Web searches is also required.

Rating systems give each Web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject these pages.

Monitoring records Internet sites visited by individual user. Access to a site forbidden by the filtering policy will result in a report. It is also possible to remove access automatically after a set number of policy violations.

Despite careful design, filtering systems cannot be completely effective due to the speed of change of Web content. Filtering may be performed by the ISP, by the LA, at school-level or by any combination. School-level systems require considerable management to maintain effectiveness and place huge responsibility on the school if they are the only systems in place.

Careful monitoring and management of all filtering systems will be required. It is important that the school establishes the filtering criteria rather than simply accepting filtering default settings.

· The school will work in partnership with parents, the LA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

· If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT Co-ordinator.

· Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

· Any material that the school believes is illegal must be referred to the Internet Watch Foundation (please see references given in support document).

· Filtering strategies will be selected by the school, in discussion with the filtering provider where appropriate.

11) How will the policy be introduced to pupils?

· A booklet on responsible Internet use will be compiled covering both school and home use and distributed to parents.

12) How will staff be consulted?

· All staff must comply with the terms of the '**Responsible Internet Use**' statement before using any Internet resource in school.

· All staff will be provided with the School Internet Policy.

· Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

· The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by senior management.

· Staff development in safe and responsible Internet use, and on the school Internet policy will be provided as required.

· Staff will sign to indicate they have read the policy.

13) How will ICT system security be maintained?

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.

· Security strategies will be discussed with the LA.

· Personal data sent over the Internet will be encrypted or otherwise secured.

· Use of portable media such as memory sticks and CD- ROMs will be reviewed. Portable media may not be brought into school without specific permission and a virus check.

· Unapproved system utilities and executable files will not be allowed in pupils' work areas..

· Files held on the school's network will be regularly checked.

14) How will complaints regarding Internet use be handled?

· Any complaint about staff misuse must be referred to the Headteacher.

· As with drugs issues, there may be occasions when the police or child protection staff must be contacted. Early contact could be made to establish the legal position and discuss strategies.

15) How will parents' support be enlisted?

· Parents' attention will be drawn to the School Internet Policy in newsletters, the school brochure and on the school Web site.

· A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.

· Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

· Interested parents will be referred to organisations such as PIN, Parents Online and NCH Action for Children (URLs in reference section).

(Staff) Responsible Internet Use Statement

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience

- Do not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application

- On-line gambling or gaming is not allowed

It is at the Headteacher's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure, and remove any portable media from computers when not attended.
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

Remote Access (staff):

- You are responsible for all activity via your remote access facility

- Only use equipment with an appropriate level of security for remote access

- To prevent unauthorised access to school systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential

and do not disclose them to anyone

- Select PINs to ensure that they are not easily guessed, eg do not use your house or telephone number or choose consecutive or repeated numbers

- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is

- Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment

Dear Parents

Use of the Internet within school

As part of your child's learning and the development of their ICT skills, Sunningdale is providing supervised access to the Internet. We believe that the effective use of the Internet and E-mail is a worthwhile part of learning for our children as they grow up in the modern world.

Although there will always be on-going concerns about children having access to undesirable materials, we have taken positive steps to reduce this risk in school. Our school Internet provider operates a filtering system that restricts access to inappropriate materials.

As part of our commitment to work in partnership with parent/carers the new policy is attached.

Should you wish to discuss any aspect of Internet use please contact school to discuss further.

Yours sincerely,

Headteacher

Responsible Internet Use Statement

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience

- Do not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application

- On-line gambling or gaming is not allowed

It is at the Headteacher's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure, and remove any portable media from computers when not attended.
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

Remote Access (staff):

- You are responsible for all activity via your remote access facility

- Only use equipment with an appropriate level of security for remote access

- To prevent unauthorised access to school systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone

- Select PINs to ensure that they are not easily guessed, eg do not use your house or telephone number or choose consecutive or repeated numbers

- Avoid writing down or otherwise recording any network access

information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is

- Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment