ST VINCENT'S SCHOOL
A Specialist School for Sensory Impairment and Other Needs

Policy Document Title:	Internet Access Policy
Updated:	10/23 SI
To be reviewed:	10/24

Who has written the policy?

The School's Internet Access Policy is part of the school's ICT Policy and the School Development Plan and will relate to other policies including those for behaviour, for personal, social and health education (PSHEE) and for citizenship.

Why is Internet access important?

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.

How does the Internet benefit education?

The Government set targets for networked Internet use in all schools by 2002 through the National Grid for Learning (NGfL) initiative. A number of studies and government projects have identified the benefits to be gained through the appropriate use of the Internet in education.

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in government initiatives such as the National Grid for Learning (NGfL) and the Virtual Teacher Centre (VTC);
- educational and cultural exchanges between pupils world-wide;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- 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;
- exchange of curriculum and administration data with the LA and DfES.

How will Internet use enhance learning?

Discussion: Increased computer numbers or improved Internet access may be provided but effective use and quality of learning must also be addressed. Developing good practice in Internet use as a tool for teaching and learning is clearly essential. Librarians and teachers need to help pupils learn to distil the meaning from the mass of information provided by the Web. Often the quantity of information needs to be cut down and staff could guide pupils to appropriate Web sites, possibly by publishing lists on the school intranet or on the school Web site for use at home. Offering pupils a few good sites may be better than suggesting the whole Web is searched!

The Kent Webskills project, amongst others, suggests ways to develop good practice in retrieving, reporting and evaluating information for research projects.

- 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 is acceptable and what is not acceptable 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 and retrieval.

How will pupils learn to evaluate Internet content?

Discussion: The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop skills in selection and evaluation. The spreading of malicious rumour has occurred for thousands of years and lies sometimes win over truth. Information received via the Web, e-mail or text message also requires good information handling skills. In particular it may be difficult to determine origin and accuracy, as the contextual clues present with books or TV may be missing or difficult to read. A whole curriculum approach may be required.

Inappropriate material should not be visible to pupils using the Web. This is not easy to achieve and cannot be guaranteed. It is a sad fact that pupils may be confronted with inappropriate material, despite all attempts at filtering. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example, to close the page and report the URL to the teacher or ICT manager for inclusion in the list of blocked sites.

More often, pupils will be judging reasonable material but selecting that which is relevant to their needs, for instance to answer a homework question. Pupils should be taught research techniques including the use of subject catalogues and search engines. They should be encouraged to question the validity, currency and origins of information – key information handling skills. They should also use alternative sources of information for comparison purposes. Looking for the author's name, date of revision and whether others link to the site is a start. Effective guided use will reduce the opportunity pupils have for exploring unsavoury areas.

Access to sensitive sites, for example those that record the Holocaust, may be required for the duration of a specific educational activity by supervised pupils of appropriate age. Some filtering software can provide temporary access to specific sites.

Using Internet derived materials in pupils' own work requires at least an understanding that straight copying is worth little without a commentary that demonstrates the selectivity used and evaluates significance. Respect for copyright and intellectual property rights, and the correct usage of published material needs to be taught. Methods to detect plagiarism may need to be further

developed.

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

The following statements will require adaptation according to the pupils' age:

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.
- Training should be available to staff in the evaluation of Web materials and methods of developing students' critical attitudes.

How will e-mail be managed?

Discussion: The government encourages the use of e-mail as an essential means of communication. Directed e-mail use can bring significant educational benefits and interesting projects between neighbouring villages and between continents have been created, often with the help of "project finder" sites. However, the use of e-mail requires that the implications for the school and for the pupils have been thought out and that appropriate safety measures have been put in place. Un-regulated e-mail can provide a means of access to pupils that bypass the traditional school boundaries.

The central question is the degree of responsibility for self-regulation that may be delegated to an individual pupil. Once e-mail is available it is difficult to control its content. Restriction of incoming and outgoing e-mail to approved addresses and filtering for unsuitable content and viruses is now possible.

In the school context, e-mail should not be considered private and most schools, and indeed firms, reserve the right to monitor e-mail. There is a balance to be achieved between monitoring that is

necessary to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

The use of personal e-mail addresses such as **john.smith@stvin.com** needs to be carefully restricted to appropriate situations; indeed the government has announced that whole-class or project e-mail addresses should generally be used in primary schools. Schools will need to decide how whole-class or even individual e-mail accounts can be managed within the staff resources available**.** It is important to appreciate the differences of operation between web-based and pop3 e-mail accounts.

Many teenagers have their own e-mail accounts, such as the web-based Hotmail, which they use widely outside school. If e-mail accounts are not monitored there is the risk that pupils could send inappropriate material. Similarly external web-based e-mail accounts with anonymous names such as **pjb354@emailhost.com** make monitoring difficult. One strategy is to limit e-mail use to accounts on the school domain or even to limit pupils' e-mail to within the school network.

Much e-mail use is purely of a social nature. Is social e-mail use considered useful experience of a communication tool or is it of low priority? Should access to social e-mail be made available only outside lesson hours?

- 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 details of themselves or others, such as address or telephone number, or arrange to meet anyone in e-mail communication.
- Whole-class or group e-mail addresses should be used at Key Stage 2 and below.
- Access in school to external personal e-mail accounts may be blocked.
- Excessive social e-mail use can interfere with learning and may be restricted.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is banned.

How should Web site content be managed?

Discussion: Many schools have created excellent Web sites that inspire pupils to publish work of a high standard. Web sites can celebrate pupils' work, promote the school and publish resources for projects or homework. Editorial guidance will ensure that the Web site reflects the school's ethos that information is accurate and well presented and that personal security is not compromised. Web and paper publication content is likely to overlap and a single editorial team would ensure common values and quality control.

Although there are many ways to obtain information about schools and pupils, for instance a school newsletter, a school's Web site can be accessed by anyone on the Internet. Publication of information should be considered from a security viewpoint. Material such as staff details or a detailed plan of the school may be better published in the school handbook or on an intranet and thereby restricted to known persons. School Web sites are often new projects and security may not have been fully considered and strategies established. For example, a password-protected Web page could give a false sense of security unless the method used is sound.

Photographs that include pupils add a liveliness and interest to a Web site that is difficult to achieve in any other way. Nevertheless the security of staff and pupils must come first. Sadly, although common in newspapers, the publishing of pupils' names with large photographs of pupils is not acceptable. Web images could be misused and individual pupils identified.

Strategies include using relatively small photographs of groups of pupils and using photographs that do not show faces at all. "Over the shoulder" can replace "passport-style" photographs but still convey the educational value of the activity. With imagination it is possible to replace many personal photographs with self-portraits or images of pupils' work or of an activity such as a science investigation. A check should be made that pupils in photographs are appropriately clothed.

Photographs of a pupil should not be published without the parent's or carer's written permission. Some schools ask for permission to publish images of work or appropriately taken photographs of pupils once per year, others at the time of use.

- The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be identified.
- Pupils' full names will not be used anywhere on the Web site, particularly associated with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- The Principal or nominee will take overall editorial responsibility and ensure 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.

Are newsgroups and chat safe?

Discussion: Conferencing is a powerful method for pupils and teachers to share information and opinion. Some conferencing applications, including chat and newsgroups sometimes attract undesirable and irrelevant comment, often from anonymous elements. Other collaboration tools such as moderated mailing lists and discussion facilities with a defined community of known users are far safer, but seem to be used less frequently. Collaboration tools are covered in detail in the "Internet Users Guide" described in the reference section.

An e-mail distribution list can be the simplest method of distributing material to a set of selected users and is reasonably secure as the sender has complete control over who may join the list.

List servers automatically send e-mail to a list of users. Lists can be private, new users are added only by the moderator or public, anybody can join the list. A useful example is UK-schools: **www.jiscmail.ac.uk/lists/uk-schools.html**

A number of respected individuals or organisations including BECTa, LAs and some ICT suppliers

run discussion groups. While the cost of hosting is low, the energy and organisation of the list or group owner / moderator is essential to keep users on topic and ensure inappropriate postings do not occur.

Newsgroups or Usenet is a method of posting messages that can later be collected by any user interested in that particular topic. Some newsgroups are highly technical and others are dedicated to particular interests or hobbies. However some are deeply disturbing. Open access to unmoderated newsgroups by contributors means that newsgroups can be infiltrated by the immature and offensive and for this reason, in general, should not be made available to pupils. Access to the information in the best newsgroups can usually be obtained through list servers and e-mail lists.

Chat is a popular conferencing application offering instantaneous exchange of text between groups of users. In principle, chat has great potential for education; for instance pupils could exchange live text, speech or video with pupils in South Africa or Italy, at low cost. Such chat facilities would be moderated by the teacher. Unauthorised persons would not know of its existence and not be able to gain access.

There are many varieties of chat including IRC, ICQ, graphical chat areas using avatars (cartoons), instant messaging and chat hosted on Web sites. Security varies widely and one has only to visit some chat rooms to be aware of the risks. Public, unregulated chat rooms could be used by the unscrupulous to gain access to pupils. Their use in school, even in a club setting, is highly debatable. Outside school, many pupils use a variety of chat facilities and may not be fully aware of the dangers.

- Pupils will not be allowed access to public or unregulated chat rooms.
- Children should use only regulated educational chat environments. This use will always be supervised and the importance of chat room safety emphasised.
- Newsgroups will not be made available unless an educational requirement for their use has been demonstrated.
- A risk assessment will be carried out before pupils are allowed to use a new technology in school.

How can emerging Internet uses be managed?

Discussion: Many emerging communications technologies offer the potential to develop new teaching and learning strategies. Mobile communications, wide Internet access and multimedia all present opportunities which need to be evaluated to assess risks, to establish benefits and to develop good practice. One approach is to deny access until a risk assessment has been completed and safety demonstrated.

Virtual classrooms and virtual communities can widen the geographical boundaries of learning. A community could be the pupils in a primary classroom sharing computers with access to each other's work and a single class e-mail address. Pupils, teaching and non-teaching staff and governors would make a larger community, which could be extended to include parents, commercial partners and even the whole LA.
The safety of virtual communities depends on users being validated by the community and clearly identifiable in all communication. This may not be easy. Should a disaffected pupil be removed from the virtual community or encouraged to use the facility for reasons of inclusion? Of course the technology itself needs to be secure, and explicitly exclude unknown users.

Within the safe community, or an appropriate sub-set of the community, the risks presented by communications facilities such as chat, e-mail and message boards become much safer. New approaches such as peer mentoring and parent access to assessment scores and can be investigated. Examples of virtual communities include the DfES's Grid Club for pupils aged 7-11 (**www.gridclub.com**) and Think.com (**www.think.com**).

Video conferencing introduces new dimensions. Cameras cost as little as £50 and, with faster Internet access, enable limited video to be exchanged across the Internet. The availability of live video can increase safety – you can see who you are talking to – but if inappropriately used, a video link could reveal security details.

New applications are continually being developed which use the Internet, the mobile phone network and wireless or infrared connections. The user could be mobile using a WAP phone or

personal digital assistant with wireless Internet access.

Schools should ensure that they are up to date with new technologies, including those relating to mobile phones and hand-held devices, and be ready to develop appropriate strategies. For instance text messaging via mobile phones is a frequent activity for many pupils. Could teachers communicate with a truanting pupil? Could reminders for exam coursework be sent by text message?

The inclusion of inappropriate language or graphical icons within text messages is difficult for staff to detect. Pupils may need reminding that such usage is both inappropriate and conflicts with school policy. Abusive text messages would come under the school Anti-bullying policy.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

How will Internet access be authorised?

Discussion: The school should allocate Internet access for staff and pupils on the basis of educational need. It should be clear who has Internet access, and who has not. Authorisation is generally on an individual basis in a secondary school. In a primary school, where pupil usage is fully supervised, all pupils in a class might be authorised as a group. As most pupils will be granted Internet access, it may be easier to manage lists of those who are denied access. Parental permission will be required in all cases - a chore that may be best organised once a year when other pupils' details are checked.

- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff leaving or the withdrawal of a pupil's access.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be informed that pupils will be provided with supervised Internet access (an

example letter for primary schools is included as an appendix).

- Secondary students must apply for Internet access individually by agreeing to abide by the Responsible Internet Use statement.
- Parents will be asked to sign and return a consent form. Please see the sample form later in this document.

How will the risks be assessed?

Discussion: As the quantity and breadth of the information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will need to address the issue that it is difficult to remove completely the risk that pupils might access unsuitable materials via the school system. It is wise to include a disclaimer such as the following.

- 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 school cannot accept liability for the material accessed, or any consequences of Internet access.
- 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 Principal will ensure that the Internet policy is implemented and compliance with the policy monitored.

How will filtering be managed?

Online safety is a whole school issue and under the PREVENT DUTY, schools are expected to ensure that children are safe from terrorist and extremist material when accessing the internet in school.

Discussion: Levels of access and supervision may vary according to the pupil's age and experience. Internet access must be appropriate for all members of the school community from youngest pupil to teacher and administrative staff. Systems to adapt the access profile to suit the pupil's age and

learning context are available. Older secondary pupils, as part of a supervised project, might need to access adult materials. For instance a course text or literary novel might include references to sexuality. Teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use should be recognised and restrictions removed temporarily.

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.

At St. Vincent's school, our children are protected via a two-tier system, incorporating proxy-based web-filtering, as well as router-based filtering and a point-of-entry firewall. This will allow monitoring and moderation/blocking of all broadband traffic. We are currently certified by the "Cyber Essentials" scheme regarding our competent level of cyber security.

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 theLA, 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 later).
- Filtering strategies will be selected by the school in discussion with the filtering provider where appropriate. Where possible, the filtering strategy will be selected to suit the age and curriculum requirements of the pupil.

How will the policy be introduced to pupils?

Discussion: Many pupils are very familiar with Internet use and culture and it would be wise to discuss the School Internet Policy with them, possibly through a student council. As pupils' perceptions of the risks will vary, the rules may need explanation and discussion. Pupils may need to be reminded of the school rules at the point of Internet use. Later in this document, 'Responsible Internet Use' rules are suggested, written for primary pupils and for secondary pupils and staff, which could be printed as posters for rooms with Internet access. A copy could also be given to parents when they are asked to consent to Internet use. Consideration must be given to who should be teaching pupils safe practice and when and how this will be taught.

- Rules for Internet access will be posted near all computer systems.
- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- A module on responsible Internet use will be included in the PSHEE programme covering both school and home use.

How will staff be consulted?

Discussion: It is important that teachers and learning support assistants are confident to use the Internet in their work. The School Internet Policy will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop

appropriate teaching strategies. It would be unreasonable, for instance, if cover staff or supply staff were asked to take charge of an Internet activity without preparation. Clarification and discussion may be required.

Staff must understand that the rules for any employee on Internet misuse are quite specific. Instances of misuse resulting in dismissal have occurred. If staff have doubts as to the legitimacy of any aspect of their Internet use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

Internet use is widespread and all staff including administration, caretaker, governors and helpers should be included in appropriate awareness raising and training. Internet use should be included in the induction of new staff, for instance in the selection of appropriate modes of expression in e-mail communication to prevent confusion. In commerce, e-mail is used extensively and is often considered to be a legal document.

- All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school. All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and its importance explained.
- 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 the safe and responsible Internet use, and on school Internet policy will be provided as required.

How will ICT system security be maintained?

Discussion: It is important to review the security of the whole system, from user practice to Internet service provider (ISP). At the simplest level, occasional checks on user's files, temporary Internet files and history files can reveal potential mischief.

Making systems secure is a complex matter and cannot be dealt with adequately in this document. A number of agencies can advise on systems security including LA support teams and suppliers. The ICT Security Policy produced by the South East Grid for Learning (SEGfL) provides further information and discussion. Local Area Network security issues include:

- The user must act reasonably. Loading non-approved software could cause major problems. Good password practice is required including logout after use.
- The workstation should be secure from casual mistakes by the user.
- Cabling should be secure and wireless LANs safe from interception.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured to a high level.
- Virus protection for the whole network must be installed and current.

Wide Area Network (WAN) security issues include:

- All external connections must be assessed for security risks including the wide area network connection and any modems staff may wish to use.
- Firewalls and routers should be configured to prevent unauthorised use of software such as FTP and Telnet at the protocol level.
- Decisions on security made by external agencies such as the LA or ISP must be discussed with schools. Third-party security testing should be considered.

The Internet is a connection to the outside world that could compromise system performance or threaten user or system security. The downloading of large files such as video and MP3 can compromise system performance. A wide area network (WAN) connection introduces further risks such as pupils trying to access another school. However it also brings the opportunity for industrial strength security in the form of hardware firewalls and the expertise to design and operate them.

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Use of floppy disks will be reviewed. Personal floppy disks 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 or attached to e-mail.
- Files held on the school's network will be regularly checked.
- The IT co-ordinator / network manager will ensure that the system has the capacity to take increased traffic caused by Internet use.

How will complaints regarding Internet use be handled?

Discussion: Parents and teachers must know how and where to report incidents. Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance whether the Internet use was within or outside school. Transgressions of the rules may be minor and can be dealt with by the teacher as part of normal class discipline. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's behaviour policy. Complaints of a child protection nature must be dealt with in accordance with child protection procedures.

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the Principal.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- As with drugs issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.
- Sanctions available include:
  - interview/counselling;
  - informing parents or carers;
  - removal of Internet or computer access for a period, which could prevent access to school work held on the system, including examination coursework.

How will parents' support be enlisted?

Discussion: Internet use in pupils' homes is increasing rapidly, encouraged by offers of free access and continual media coverage. Unless parents are aware of the dangers, pupils may have

unrestricted access to the Internet. The school may be able to help parents plan appropriate, supervised use of the Internet at home. One way might be to help parents to understand more about ICT themselves - perhaps by running courses for them (although the implications for resources will need to be considered).

Schools may wish to refer parents to sites such as PIN and NCH / European Research into Consumer Affairs (see references at the end of the document).

- Parents' attention will be drawn to the School Internet Policy in newsletters, the school brochure and on the school Web site.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- 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.
- A stock of relevant leaflets from organisations such as BECTa, PIN, and NCH Action for Children will be maintained.

How is Internet used across the community?

Discussion: The Internet is used in many situations in the local community. In addition to the home, access may be available at the local library, youth club, adult education centre, village hall, supermarket or cyber café. The school may wish to contact their community colleagues in order to advise pupils regarding booking procedures, availability and possible costs.

In community Internet access there is a fine balance to be achieved in ensuring 'freedom of information' whilst providing adequate protection for children and others who may be offended by inappropriate material. Each organisation is developing access appropriate to its own client groups and pupils may find variations in the rules and even unrestricted access to the Internet. Although policies and practices may differ, community partners adhere to the same laws as schools with respect to content, copyright and misuse. Staff may wish to exchange views and compare policies with others in the community. Where rules differ, a discussion with pupils on the

reasons for the differences could be worthwhile.

Sensitive handling of cultural aspects is important. For instance filtering software should work across community languages and school Internet policies may need to reflect the pupils' cultural backgrounds. Assistance from the community in drawing up the policy could be helpful.

Example of Libraries Internet access rules:

- Adult users will need to sign the acceptable use policy.
- Parents/carers of children under 18 years of age will generally be required to sign an acceptable use policy on behalf of the child.
- In libraries, children under 8 years of age must be accompanied by an adult when accessing the Internet.

St Vincent's School for Blind and Partially Sighted Children
Responsible Internet Use

Rules for Staff and Students

The school computer system provides Internet access to students and staff. This Responsible Internet Use statement will help protect students, staff and the school by clearly stating what is acceptable and what is not.

- Access must only be made via the user's authorised account and password, which must not be given to any other person.
- School computer and Internet use must be appropriate to the student's education or to staff professional activity.
- Copyright and intellectual property rights must be respected.
- Users are responsible for e-mail they send and for contacts made.
- E-mail should be written carefully and politely. As messages may be forwarded, e-mail is best regarded as public property.
- Anonymous messages and chain letters must not be sent.
- The use of public chat rooms is not allowed.
- The school ICT systems may not be used for private purposes, unless the headteacher has given permission for that use.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- The security of ICT systems must not be compromised, whether owned by the school or by other organisations or individuals.
- Irresponsible use may result in the loss of Internet access.

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

Responsible Internet Use

We use the school computers and Internet connection for learning.

These rules will help us to be fair to others and keep everyone safe.

- **I will ask permission before entering any Web site, unless my teacher has already approved that site.**
- **On a network, I will use only my own login and password, which I will keep secret.**
- **I will not look at or delete other people's files.**
- **I will not bring floppy disks into school without permission.**
- **I will only e-mail people I know, or my teacher has approved.**
- **The messages I send will be polite and sensible.**
- **When sending e-mail, I will not give my home address or phone number, or arrange to meet someone.**
- **I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.**
- **I will not use Internet chat.**
- **I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.**
- **I know that the school may check my computer files and may monitor the Internet sites I visit.**
- **I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers.**

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mail and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

Dear Parents

Responsible Internet Use

As part of your child's curriculum and the development of ICT skills, St. Vincent's School is providing supervised access to the Internet. We believe that the use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the attached Rules for Responsible Internet Use and sign and return the consent form so that your child may use Internet at school.

Although there have been concerns about pupils having access to undesirable materials, we are taking positive steps to deal with this risk in school. Our school Internet provider operates a filtering system that restricts access to inappropriate materials. This may not be the case at home and we can provide references to information on safe Internet access if you wish. We also have leaflets from national bodies that explain the issues further.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable for any damages arising from your child's use of the Internet facilities.

Should you wish to discuss any aspect of Internet use (or to see a lesson in operation) please telephone me to arrange an appointment.

Yours sincerely

Consent Form

Gaining pupils' and parents' agreement to the Rules for Responsible Internet Use is important but requires sound organisation. Some schools do this once each year, at the same time as checking the home and emergency contact details. The Rules for Responsible Internet Use should be included with the letter to parents to avoid any misunderstanding.

For pupils above the age of 16 and not living at home or for pupils18 or older, the school should be able to rely on the consent of the pupil alone. Otherwise parent's consent must be obtained. It is also wise to obtain parent's permission to publish pupil's work and to publish pupil's photographs, subject to strict safeguards, on the school Web site.

Responsible Internet Use

Please complete, sign and return to the school secretary

Pupil:	***Form:***
Pupil's Agreement I have read and understand the school Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times.	
Signed:	***Date:***
Parent's Consent for Internet Access I have read and understood the school rules for responsible Internet use and give permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.	
Signed:	***Date:***
Please print name:	
Parent's Consent for Web Publication of Work and Photographs I agree that, if selected, my son/daughter's work may be published on the school Web site. I also agree that photographs that include my son/daughter may be published subject to the school rules that photographs will not clearly identify individuals and that full names will not be used.	
Signed:	***Date:***

Based on the Internet Policy of the Irish National Centre for Technology in Education.