



Est. 1905

CHISWICK HOUSE SCHOOL



ST MARTIN'S COLLEGE

ACCEPTABLE COMPUTER USE

AND

INTERNET ACCESS POLICY

© 2004 - Jason R Cutajar

This Policy has been based on the Internet Policy established at
© **Kent County Council**
and other articles from the British NGFL Superhighway Safety
and the Information Systems - Acceptable Use Policy of the Education Division, Malta.



*Acceptable Computer Use and Internet Access Policy for
Chiswick House School and St. Martin's College*

Table of Contents

Rationale 3

Terminology..... 4

Importance and Benefits of Internet Use 5

Acceptable Use - Definition 5

Acceptable Use Policy for Internet Access 6

Privileges 6

Staff & Student Web Pages 6

Netiquette 6

Privacy 6

Responsibility..... 7

The Internet as a tool to enhance learning 7

Students as effective users 7

E-Mail..... 8

The School Web-Site 8

Newsgroups & Chat..... 9

Management of Internet Use..... 9

Risks..... 9

System Security 10

Management of ICT system security..... 10

Vandalism..... 11

Complaints Handling 12

Parents' Support 12

Internet Use Guidelines for Students, Teachers and Visitors 13



RATIONALE

The new NMC puts more stress on the use of ICT throughout the curriculum and the Internet is one of the latest tool available for teachers to teach and for students to learn. As an educational institution it is imperative that we equip the students with the necessary skill to use data communication effectively. An Internet Policy should provide the framework how this should be achieved while safeguarding all stakeholders.

The Internet is an open communications channel, available to all. Applications such as the Web, e-mail and chat all transmit information over the wires and fibres of the Internet to many locations in the world at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Some of the material is published for an adult audience and is unsuitable for pupils. In addition, some use the Web to publish information on weapons, crime and racism that would be more restricted elsewhere. Sadly e-mail and chat communication could also provide opportunities for adults to make contact with children for inappropriate reasons. In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and a need to teach them to be aware of and respond responsibly to the risks.

Schools need to protect themselves from possible legal challenge. The legal system is still struggling with the application of existing decency laws to computer technology. It is clearly an offence to hold images of child pornography on computers but the possession of other obscene or offensive materials is not clearly covered. Schools can help protect themselves by making it clear to users that the use of school equipment to view or transmit inappropriate material is "unauthorised". However, schools should be aware that a disclaimer does not protect a school from a claim of death or personal injury and the school needs to ensure that all reasonable and appropriate steps have been taken to protect pupils.

Teachers will be aware of the risks of Internet use but may have had few opportunities for detailed discussion. Advice and training from advisers or child protection officers should be sought. Policy writing provides an opportunity for discussion and a policy agreed by staff will be easier to implement than one imposed.



TERMINOLOGY

The Internet is a huge network of computers making a worldwide community, with millions of members, providing a vast store of information with great possibilities for education. More than 80% of all primary schools, all colleges and virtually all secondary schools already have an Internet connection and the Government's target is for all schools, colleges and libraries to be connected. The home user market is also expanding at a very fast pace.

The Internet offers a range of facilities, allowing users to obtain information and resources, to communicate with each other and to publish information. Some of the most frequently used facilities include:

The World Wide Web (WWW) or Web provides easy access to the vast quantity of information and resources available on the Internet and is the facility which people use to 'surf' for information. It is made up of millions of screens, or 'pages', of information. The collection of pages created by one individual or organisation is known as a website. Each page can include text, images, sound, animation and video and has its own unique address.

E-mail allows users to send and receive written messages via a telephone line. Students have used e-mail for communicating with pen pals, to send questions to a specialist (such as a vulcanologist) to help with project work, and to swap information, for example, about their locality and weather with students in other countries.

Mailing lists usually consist of a group of people who exchange e-mail about a subject that interests them.

Internet Service Providers (ISPs) provide the link between the user and the Internet. Some provide a free service and with others, charges vary according to the type of connection, amount of use and additional services such as filtering.

Newsgroups are like international noticeboards where people log in to a particular group to read and contribute remarks or questions. There are thousands of newsgroups covering any and every topic and interest, including some which could be considered offensive.

Consequently, some ISPs choose not to offer their subscribers all groups, or do not carry news at all. Nonetheless, older students have benefited from access to newsgroups, which have helped to expand their knowledge and allowed them to discuss specific topics in depth.

Chat rooms allow a number of people to 'meet' on the Internet and have live, 'real-time' conversations. It is similar to having a telephone conversation with a number of people at once except that the participants type instead of talk. Open chat lines are not often used in schools, to avoid any possible compromise to pupil safety. However, chat rooms are very popular with pupils who have on-line access at home.



Video conferencing enables two or more people, in different locations, to see one another while they talk. Secondary schools, in particular, have used video conferences as a resource for language learning, for example. It is also possible to arrange for the exchange of audio, video, images or any other digital file to allow users in different places to work concurrently on the same resource.

IMPORTANCE AND BENEFITS OF INTERNET USE

On designing an Internet Policy, the most important question relies on the benefits achieved in using the Internet through this policy. This policy provides the following purposes.

- *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.*
- *Internet access is an entitlement for students who show a responsible and mature approach to its use.*
- *The Internet is an essential element in 21st Century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.*

ACCEPTABLE USE - DEFINITION

Accessing the Internet must be in support of education and research and within the educational goals and objectives of the Schools. Use of Internet will take place under the supervision of the teacher and students are personally responsible at all times when using the electronic information service. Transmission of any material in violation of the Maltese law, or school policy is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material, or materials protected by trade secret. Commercial activities by/for profit institutions are not acceptable. Use of product advertisement or political lobbying is prohibited. Any action which interferes with the intended use of the system, violates another person's right to privacy, including the following: reposting personal communications without an author's consent, giving out names, addresses, phone numbers or passwords of others or trespassing in another person's account is also prohibited. Attempting to gain unauthorized access to the system or network resources, downloading, storing or printing files or messages that are profane, obscene or contain inappropriate language, transmitting or causing to be transmitted, any communication that could be construed as harassment or disparagement of others is also inappropriate. Using the network for financial or commercial gain, wasting resources by failing to monitor personal files, illegally installing copyrighted software on school computers, subscribing to list servers and/or newsgroups without prior approval of a school official, or accessing the Internet Relay Chat area are also forbidden.



ACCEPTABLE USE POLICY FOR INTERNET ACCESS

The Schools have made content-filtered Internet access available to students, and staff, providing users with access to thousands of worldwide computer networks which contain a vast array of educational resources. These will strengthen the communicative and research skills of students and significantly expand their knowledge base.

PRIVILEGES

The use of the information systems is a privilege, not a right, and inappropriate use will result in cancellation of those privileges. The school administrators will deem what is inappropriate use and their decision is final. The School administrators may disallow the use of information systems at any time as required.

STAFF & STUDENT WEB PAGES

The School may provide web space to students and staff. Publication of any material in violation of the Maltese law, or school policy is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material, or materials protected by trade secret. Commercial activities by/for profit institutions are not acceptable. The Schools will constantly monitor the content on web pages they host and reserve the right to withdraw web space and take disciplinary action against users in breach of its acceptable use policy.

NETIQUETTE

All users are expected to adhere to the generally accepted rules of network etiquette. These include but are not limited to the following: Be polite. Do not get abusive in your messages to others. Use appropriate language. Illegal activities are strictly forbidden. Do not reveal the personal address, phone number or credit card number of students or colleagues. Note that, e-mail is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities. Do not use the network in such a way that would disrupt the use of the network by other users. All communications and information accessible via the network should be assumed to be private property.

PRIVACY

Schools may publish selected students' work and photographs that include students with the respective parents' written consent.



RESPONSIBILITY

The Schools make no warranties of any kind, whether expressed or implied for the service it is providing. The Schools will not be responsible for any damages you suffer. This includes but not limited to : loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence or user errors or omissions. The Schools specifically deny any responsibility for the accuracy or quality of information obtained through its services.

THE INTERNET AS A TOOL TO ENHANCE LEARNING

The effectiveness of the implementation of this Internet Policy relies on the teachers and their teaching strategies. Teachers can use the internet as a tool to :

- *access to world-wide educational resources including museums and art galleries;*
- *inclusion in government initiatives such as the E-Government concept.*
- *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;*

STUDENTS AS EFFECTIVE USERS

Students can only become effective users if the school provide for the following strategies :

- *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.*



E-MAIL

Data communication is an integral part of this policy and we should stress the use of data communication not only for educational purposes but also for administration purposes.

Use of School provided e-mail must be in support of education and research. Electronic mail is not guaranteed to be private. System administrators reserve the right to access e-mail to investigate complaints. Under these circumstances, messages which are found to be in violation of acceptable use will be reported to appropriate personnel. All messages sent are traceable to the user and logs of transactions are maintained and can be used to monitor use.

- *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.*
- *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.*

THE SCHOOL WEB-SITE

A school web-site would form part and parcel of this policy. The school web-site too needs some sort of regulations especially when publishing children material and photos on the web.

- *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 headteacher 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.*

NEWSGROUPS & CHAT

Probably the less regulated tools used over the Internet. A strategy to minimize the risk in these areas is a must as more often than not these tools are abused rather than used.

- *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.*

MANAGEMENT OF INTERNET USE

As we are nearing to provide Internet access in the Library, a need to develop some sharing of responsibilities is a must. Access to the Internet should not be solely from the computer labs but very soon from every class.

- *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 Junior Stage, 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.*

RISKS

- *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. Neither the school nor the teachers can accept liability for the material accessed, or any consequences of Internet access.*
- *Methods to identify, assess and minimise risks will be reviewed regularly.*
- *The headteacher will ensure that the Internet policy is implemented and compliance with the policy monitored.*



SYSTEM SECURITY

Security on any computer is a high priority, especially when the system involves many users. If you feel you can identify a security problem on the Internet, you must notify a school administrator. Do not demonstrate the problem to other users. Attempts to logon to the network as a system administrator will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to information systems.

Filtering systems prevent or block users' access to unsuitable material. When the filtering system is turned on, users cannot open or link to sites that the filtering system recognises as unsuitable. Although a useful tool, filtering systems are not foolproof. They should not replace vigilance or simple common sense from network administrators, teachers or parents.

Filtering content is just one way of making sure that children do not access inappropriate material. Schools need to consider the other ways of ensuring pupils do not have access to inappropriate material. Schools also need to monitor what pupils are logging on to. The schemes of work for ICT include teaching pupils to question the source of web material. Teachers need to equip learners with the skills to become discriminating users of the internet.

Pupils, staff and parents should sign up to an Acceptable Use Policy and there should be clear sanctions if your approach is to be effective.

- *The school will work in partnership with parents 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.*
- *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.*

MANAGEMENT OF ICT SYSTEM SECURITY

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.



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.
- 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.*
- *Security strategies will be discussed with the LEA, particularly where a wide area network connection is being planned.*
- *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.*

VANDALISM

Vandalism will result in cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy data or equipment of another user, or of any of the agencies providing Internet access. This includes but is not limited to the uploading, downloading, sharing or creation of computer viruses, worms, trojans or any other malicious code.

COMPLAINTS HANDLING

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 headteacher.*
- *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 by head;*
 - *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.*

PARENTS' SUPPORT

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).

- *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.*



INTERNET USE GUIDELINES FOR STUDENTS, TEACHERS AND VISITORS

Responsible Internet Use Rules for Staff and Students

- The school computer system provides Internet access to students, staff and visitors. This Responsible Internet Use statement will help protect students, staff, visitors 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.
- I will ask permission before entering any Web site, unless my teacher has already approved that site.
- 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.
- 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 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. The use of public chat rooms is not allowed.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- 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.
- 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.
- 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.

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.