

# Stanbridge Earls School

## ICT Policy

25<sup>th</sup> May 2006

**WHEN USING STANBRIDGE EARLS SCHOOL INFORMATION AND COMMUNICATIONS TECHNOLOGY EQUIPMENT THERE SHOULD BE NO EXPECTATION OF PRIVACY. STANBRIDGE EARLS SCHOOL CLEARLY STATES THAT IT WILL MONITOR THE USE OF THESE SYSTEMS.**

### Definition of Unsuitable and Inappropriate

DO NOT send, receive, download, display, print or distribute material that is: -

- Sexually explicit
- Obscene
- Likely to cause complaints of sexual or racial harassment
- Intimidating
- Fraudulent
- Defamatory
- Otherwise unlawful

### Prohibited Activities

The following uses of the Internet are specifically prohibited and will be dealt with as serious breaches of the school's ICT Policy.

- Accessing web pages by writing in the numerical IP address
- Accessing Ebay or any other auction websites
- Using MSN Messenger
- Accessing any chat room websites

# **1. E-Mail**

## **Introduction**

Stanbridge Earls School encourages staff and pupils to send e-mails instead of letters, faxes and other forms of paper communications where deemed appropriate. This form of contact provides quicker communication and also a convenient way of filing such documents.

E-mail accounts will be supplied to all computer users.

Attached to this document are Guidelines for E-Mail Etiquette.

Please be aware that the system is automatically checked to protect against viruses, identifying the access of unsuitable material and for highlighting other illegal or inappropriate behaviour (Definition above). Disciplinary action may result if anyone is found to be involved in such activities. Although the system is checked this is not always sufficient, extra precautions are needed, please refer to section 1.6

## **E-mail Usage**

1.1. E-mail should be used: -

- In place of correspondence where a letter or fax may have otherwise been used.
- To send a document as an attachment so as to transmit the document quicker than by fax and in a form ready for further amendment by the recipient.

1.2. E-mail should not be used: -

- Sending unsolicited emails.
- Any form of harassment.
- Creating or forwarding chain letters or spam.

### 1.3. Reading of E-mails

- All e-mails should be read regularly.

### 1.4. Archiving

- All e-mails can be stored in a folder structure, outside of the In-Box. It is advisable to archive all e-mail for possible future reference unless the subject matter is unlikely to be referred to again. If you are unsure how to do this then please contact the ICT Department.

### 1.5. Content

- The content of all messages sent must be considered and checked, as you would do for a physical document. Please be aware that in the same way that the e-mail server protects against viruses, all contents of e-mails, both inbound and outbound will automatically be searched for inappropriate or offensive material. This will include abusive language and file attachments that are either programs or pictures. If an e-mail is sent or received with suspect content then it will be quarantined until the e-mail is checked.
- If any e-mail is found to have such content then the relevant recipient and sender will be notified that the e-mail has been quarantined. Disciplinary action may result in such circumstances.

### 1.6. Virus Protection

- Never open a document or file attachment on an incoming e-mail unless you know the sender and you know they have a bona fide reason for sending the attachment. Modern day Word Processors contain very powerful macro languages which are capable of destroying all sources of data on the Network! If you receive e-mails with attachments and are unsure if you should open them please contact the ICT Department immediately.

- All e-mails are checked for viruses.

Protecting the integrity of Stanbridge Earls School computer systems is of paramount importance.

### 1.7. Other E-mail Issues

- A member of the School who receives unsolicited e-mail must immediately notify the sender that such e-mails are not permitted, must not be sent in the future and will be deleted unread.
- A member of the School must not say anything in an e-mail that he/she would not be prepared to say in a letter (on the School's headed paper) sent to the same person.

## **2. Internet**

The Internet provides access to information on every conceivable topic. It is largely unregulated and the quality and content of information taken from it is equally unregulated.

Stanbridge Earls School encourages the use of the Internet where it provides a cost effective means of gathering relevant information and for the purchasing of some goods and services.

### Internet Usage

#### 2.1. Who may access the Internet?

- Currently Stanbridge Earls School is connected to the Internet via an ADSL line in the ICT Suite. All members of the School who have signed the agreement are allowed access to the Internet.
- All Internet use will be logged and access to many web sites will automatically be barred. Stanbridge Earls School does not expect its staff or pupils to visit any inappropriate sites and if you are in any doubt about the validity of a site please contact the ICT Department.

- Visiting inappropriate and offensive sites will be treated as misconduct and disciplinary action may be taken against any person caught abusing the system.

## 2.2. Security

- We have a Firewall system that helps reduce the risk from Hackers. As you visit a site the computer hosting that site will be able to communicate with our systems. You should, therefore, use discretion as to which sites you visit.
- Do not open a connection and leave it open, log off as soon as you have finished.

## 2.3. Downloading Files

- Most viruses now originate from the Internet. In most cases the downloading of files is not required; printing text from the Internet should be used in most cases.
- Where there is a need for downloading a file, such as a PDF file please keep this to a minimum so to avoid risk associated with this. Downloading of files such as screen savers and other non-school related files and programs is not acceptable and disciplinary procedures may follow such downloads.

# **3. Server Usage**

## **3.1. Files and Directories**

- Keep file and directory names meaningful, you may know what the contents are but may forget.
- Keep all files on the server, this is more secure than your local drive and the server is backed up every night. If you keep files on your local drive then this will be your responsibility. Your local drive is insecure.

- Regularly perform housekeeping on your files and directories, delete unwanted files and check that the files are in the correct directory.
- Try and create a hierarchy for your directories, it is far better to have ten directories with ten files in rather than one with a hundred, this will obviously depend on the content of these files.
- Do not use floppy disks for storage of information, they are vulnerable, floppy disks are regularly corrupted and the data is insecure. Floppy disks also spread viruses.
- Floppy discs may be used to transfer information from a computer in the ICT department to a computer in another location or vice versa but beware that the disc may be corrupted in transit.
- Everyone will have a personal directory. Although under normal circumstances the ICT Department will not allow access to these directories users must be aware that Stanbridge Earls School reserves the right to review what is in these directories for security and legal reasons.

### 3.2. Usernames, Passwords and Security

- You will be issued a username and password. This is to be kept very secure.
- Do not give your password to anyone else. If you do and that person does something that they shouldn't when logged in as you, you are responsible, as you should have not given your password.
- Passwords will be required to access the system in the ICT Suite.
- Do not write the password down or keep it in a computer file.

- Passwords should be changed regularly. As a guideline, a change should be considered every 4 weeks.
- If you suspect other persons have your password then please change it or contact the ICT Department to change it.
- The ICT Department does not know anyone's password and we will NOT change it to allow other people access to your files without written permission from the specific user.
- You will only have access to information on the server that has been deemed appropriate to you. If you think you need other information the ICT Department will discuss this with you.
- Report any suspected security violations or weaknesses.

### 3.3. Unauthorised Software

- No unauthorised software is to be loaded. Do NOT bring games, screen savers etc in and try and load them.
- If you require anything in addition to what is loaded then contact the ICT Department.

### 3.4. Viruses

- A Virus Shield is installed, although this will increase the protection, please be on guard for any suspicious e-mails etc. If you are in doubt then contact the ICT Department. The latest antivirus files downloaded every day.

#### **4. Other Issues**

- Log off at the end of each session. Do not shut down your computer unless instructed by a member of staff.
- Before leaving your desk check that the logging off procedure has completed.
- Do not record or process any information which knowingly infringes any patent or breach any copyright.

Disciplinary action may be taken if the policy is not adhered to.