

## SCHOOL ICT POLICIES

### COMPUTER SERVICES DEPARTMENT

#### *Global ICT Policy*

This document is about securing a network and computing systems to a reasonable and economically feasible degree against unauthorized access and/or abuse, while making them accessible for authorized and legitimate users. This responsibility includes informing users of expected standards of conduct and the punitive measures for not adhering to them. Any attempt to violate the provisions of this policy will result in disciplinary action in the form of temporary revocation of users' accounts, regardless of the success or failure of the attempt. Permanent revocations can result from disciplinary actions taken by the SMT according to network abuses investigations.

The users of the network are responsible for respecting and adhering to internal policies. Any attempt to break those policies through the use of the network may result in litigation against the offender by the proper authority of the SMT.

#### **General computing policy**

- Don't use the school network for commercial or proprietary work. Use of facilities and/or services for commercial purposes is prohibited.
- Forgeries and spoofing are not approved behavior.
- Para assistência técnica utilize os formulários próprios ou e-mail (escrevendo no assunto: subject e mencionando depois o seu nome, departamento, sala e uma breve descrição do problema)

#### **Network security policy**

- Once a user receives a userID to be used to access the network and computer systems on that network, they are solely responsible for all actions taken while using that userID.
- Applying for an userID under false pretences is a punishable disciplinary offense.
- Never give your userID or password to another person. System administrators that need to access your account for maintenance or to correct problems will have full privileges to your account.
- Sharing your userID with any other person is prohibited. In the result that you do share your userID with another person, you will be solely responsible for the actions that other person appropriated.
- Do not blame the system administrator for the behaviour of the system users.
- Deletion, examination, copying, or modification of files and/or data belonging to other users without their prior consent is prohibited.
- Continued impedance of other users through mass consumption of system resources, after receipt of a request to cease such activity is prohibited.
- Use of systems and/or networks in attempts to gain unauthorized access to remote systems is prohibited.
- Use of systems and/or networks to connect to others systems, in evasion of the physical limitations of the local/remote system, is prohibited.
- Intentional attempts to "crash" network systems or programs are punishable disciplinary offenses.
- Any attempts to secure a higher level of privilege on network systems are punishable disciplinary offenses.



- The wilful introduction of computer “viruses” or other disruptive/destructive programs into the school network or into external networks is prohibited.
- The copying of system files is prohibited.
- Using Win2k Group Policies, the following security settings have been implemented: Disable task manager, Disable lock computer, Disable change password, Disable add/remove programs, Hide background tab, Disable changing wallpaper, Hide appearance tab, Hide screen saver tab, Disable deletion of printers, Disable addition of printers, Remove properties from My Computer context menu, Hide My Network Places icon on desktop, Prohibit user from changing My Documents path, Disable adjusting desktop toolbars, Don't saving settings at exit, Disable active desktop, Disable active desktop wallpaper, Disable and remove links to windows update, Remove help menu from Start Menu, Remove run menu from Start Menu, Add logoff to Start Menu, Do not keep history of recently opened documents, Disable user tracking, Removes the folders options menu item from the Tool Menu.

### **Password security policy**

- Maximum password age: 90 days
- Account lockout threshold: 5 invalid logon attempts
- Account lockout duration: 30 minutes
- Reset account lockout counter after: 30 minutes

### **Internet security policy**

- Security Zones and Content Ratings (Win2k GPO security policy): content advisor from ICRA (Internet Content Rating Association) filtering: language, nudity, sex, violence.
- The installation of “CensorNet” (Linux platform) is currently underway, which filters content received across the Internet. The whole structure is targeted for completion by April 2005.
- The following options have been disabled from File Menu in Internet Explorer: File Save As, Save As Web Page Complete, Full Screen Menu, Save this program to disk.

### **Electronic mail policy**

- Whenever you send electronic mail, your name and userID are included in each mail message. You are responsible for all electronic mail originating from your userID.
- Forgery or attempted forgery of electronic mail messages is prohibited.
- Attempts to read, delete, copy, or modify the electronic mail of other users are prohibited.
- An attempt at sending harassing, obscene and/or other threatening email to another user is prohibited.
- Attempts at sending unsolicited junk mail, “for-profit” messages or chain letters are prohibited.
- The content and maintenance of a user’s electronic mail box is the user’s responsibility.
- Keep messages remaining in your mailbox to a minimum.

### **Disk quotas policy**

- Users should delete unwanted files immediately since they take up disk space. As well file access and network resources will reduce the speediness with the amount of data stored in the Server Hard Disk
- Your files may be accessible by persons with system privileges, so do not maintain anything private in your Server disk storage area.
- Keep files to a minimum. Files can be burned to a: CD, DVD, diskette, etc.
- The content and maintenance of a user’s disk storage area is the users responsibility.
- Attempts to evade or change resource quotas are prohibited.
- The Nature of the data stored in the personal folders in the Server it is user responsibility



- Unauthorised games, mp3 files, AVI files, MPEG files, JPEG files, all kind of compressed files, executable files and all kind of unsupported files will be removed from the Server without previous warning.
- Each user it is responsible for its own data: security and violation (giving the password to someone else means less security)
- If a user needs for a period a big amount of Hard Disk space in the Server or to store unauthorized format files it should request authorization to the ICT Department
- Foram estabelecidas as seguintes quotas de disco no servidor aplicadas a shares utilizando o software Quota & File Sentinel: Admin (5GB), Wings (6GB), Year 13 (3GB), Year 12 (3GB), Year 11 (2,5GB), Year 10 (2GB), Year 9 (1,5GB), Year 8 (1GB), Year 7 (750MB) e Year 6 (750MB).
- Os seguintes tipos de ficheiros fazem parte de uma lista de ficheiros não autorizados: \*.exe, \*.mp3, \*.com, \*.avi.
- Os ficheiros que fazem parte da lista de ficheiros não autorizados foram restringidos através de uma politica aplicada a shares utilizando o software Quota & File Sentinel.

### **Hardware policy**

- Any unauthorized, deliberate action which damages or disrupts a computing system, alters its normal performance, or causes it to malfunction is a violation regardless of system location or time duration.
- Any ICT equipment that it is not in use must be communicated to the ICT Department
- It is not allowed to move equipment from its original place, even if it is broken or not connected, without informing the ICT Department.
- Do not attempt to repair equipment on your own. Contact the ICT technical staff.
- It is not allowed to take equipment home without authorization from the ICT Department
- If anyone brings personal equipment to the school (e.g. Printer, Computer, etc) it should communicate this situation to the ICT Department.
- All ICT equipment inside the school it is not property of a Department/Section but belongs St. Julian's School

### **Software policy**

- All software installed on school computers must be licensed to the school. The Principal must approve all purchasing of software for school computers in order to avoid the purchase of more than one copy of the same program (multi-licenses are cheaper).
- All unauthorized software will be removed from computers without warning (including freeware versions).
- Beta versions are not allowed on computers unless the Principal authorizes them.
- Single copy programs running on a multi-user environment is not legal.
- Software having only one license may not be installed on more than one computer.
- Software installed on computers is the property of the school.
- No personal software can be installed on the school computers without authorization from the Principal
- Personal software for installation on school computers will have authorization for a temporary basis only and must be removed after use.
- No software in any form (freeware, Beta versions, etc.) can be downloaded from the Internet.
- Respect the copyright on material that you reproduce. The copying of copyrighted materials, such as third-party software, without the express written permission of the owner or the proper license, is prohibited.

## **Backup policy**

- Os backups são realizados todos os dias da semana e da seguinte forma: Monday - Backup incremental; Tuesday - Backup incremental; Wednesday - Backup incremental; Thursday - Backup incremental and Friday - Full backup.
- Serão guardados em backup todos os dados (pastas e ficheiros) que estejam disponíveis nos discos dos servidores de rede até á hora do backup.
- O administrador da rede não pode ser responsabilizado pela impossibilidade de restauro de pastas ou ficheiros que não estejam disponíveis nos discos dos servidores á hora do backup.
- Os backups são realizados com o software Veritas BackupExec em tapes do tipo DLT IV e estão agendados para começarem ás 23 horas.
- Os backups mensais e anuais ficam guardados no cofre da Water Tower Piso 2 e só podem ser acedidos por ICT staff ou SMT members.
- O último backup de cada mês fica guardado durante o período de 1 ano. O último backup de cada ano escolar fica guardado durante o período de 3 anos.
- At the end of the academic year, all data stored in the Server will be recorded into a CD-ROM and it will be available for consulting from the ICT Department

## **Anti Virus security policy**

- Instalada a solução cliente/servidor Symantec Norton AntiVirus Corporate edition 8.1: updates automáticos diários das definições de anti-virus no servidor e distribuídas automaticamente por todos os computadores da rede.
- Software anti-spyware: Lavasoft AdAware Se. Durante o mês de Fevereiro será instalada a solução MS Anti-Spyware

## **General procedures**

- i) The school office could contact The ICT technical staff whenever a new student is enrolled and provide her/his name, surname, year group and form tutor's name. The ICT technical staff would issue the individual user name and password and pass it on to the form tutor involved.
- ii) Students who forgot or want to change their password should be sent to me.
- iii) The Admin could contact the ICT technical staff whenever a new member of staff is contracted and provide her/his name, surname and department. The ICT technical staff would issue the individual user name and password and pass it on to department involved.

## **The Ten Commandments for computer ethics (CEI - Computer Ethics Institute)**

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not use or copy software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you write.
10. Thou shalt use a computer in ways that show consideration and respect.

## **Provisional Network policy for Students**

### **Electronic network use guidelines for students**

The use of your network account is a privilege, not a right, and inappropriate use will result in disciplinary action taken by the St Julian's School. Student's activities while using the network in our school must be in support of education and research. In addition, a student accessing the network from a school computer is responsible for all online activities, which take place through the use of her/his account. Usage will be closely monitored and inappropriate use could result in your access being terminated.

### **Acceptable Uses of the Network**

- All activities which support learning and teaching at St Julian's School.
- Users are encouraged to develop uses which meet their individual needs and which take advantage of the network's functions: electronic conferences, bulletin boards, databases, and access to the Internet.
- KS4, KS5 and staff are encouraged to use USB pen drives to transfer files to and from the network.

### **Unacceptable Uses of the Network**

- Applying for a userID under false pretences.
- Sharing your userID with any other person is prohibited. In the event that you do share your userID with another person, you will be solely responsible for the network actions of that other person.
- Deletion, examination, copying, or modification of files and/or data belonging to other users without their prior consent is prohibited and is considered unauthorized access.
- Vandalising network resources, including the uploading or creation of computer viruses. The wilful introduction of computer viruses, spyware or other disruptive/destructive programs into the school network or into external networks is considered a serious offence.
- Using impolite, abusive, or obscene language.
- Using the network in ways that violate Portuguese or EU laws.
- Activities which cause congestion of the network or otherwise interfere with the work of other users.
- Intentional attempts to "crash" network systems or programs.
- Using the network for commercial purposes or financial gain.
- Sending or receiving copyrighted materials without permission.
- Using the network for sending or retrieving obscene materials.
- Break security and/or authentication measures.
- Using the system and/or network to connect to others systems evading the physical limitations of the local/remote system.
- Falsifying one's identity to others while using the network.
- Installation of unauthorized software on the network.
- Use of network resources to commit forgery, or to create a forged instrument.

### **St Julian's Electronic mail policy**

- Whenever you send electronic mail, your name and userID are included in each mail message. You are responsible for all electronic mail originating from your userID.
- Forgery or attempted forgery of electronic mail messages is prohibited.
- Attempts to read, delete, copy, or modify the electronic mail of other users are prohibited.
- An attempt to send harassing, obscene and/or other threatening email to another user is considered a serious offence.
- Attempts to send unsolicited junk mail, "for-profit" messages or chain letters is prohibited.



- The content and maintenance of a user's electronic mail box is the user's responsibility.
- Keep messages remaining in your mailbox to a minimum.

### **Software policy**

- All software installed in school computers must be licensed to the school. The headteacher must approve all purchasing of software for school computers in order to avoid the purchase of more than one copy of the same program (multi-licenses are cheaper).
- All unauthorized software will be removed from computers without warning (including freeware versions).
- Beta versions are not allowed in school computers unless the headteacher authorizes them.
- Single copy programs running on a multi-user environment are not legal.
- Software having only one license may not be installed in more than one computer.
- No personal software can be installed on the school computers without authorization from the headteacher.
- Personal software for installation on school computers will have authorization for a temporary basis only and must be removed after use.
- Software installed in school computers is the property of the school.
- Respect the copyright of material that you reproduce. Copying copyrighted materials, such as third-party software, without the express written permission of the owner or the proper license, is prohibited.

### **Disk quotas policy**

- Users should delete unwanted files immediately as they take up disk space.
- Your files might be accessible to users with system privileges, so do not maintain anything private in your Server disk storage area.
- Keep files to a minimum as the content and maintenance of a user's disk storage area is the user's responsibility. Files can be copied to USB pen drives and floppy disks, or burnt onto CDs and DVDs.
- Attempts to evade or change resource quotas are prohibited.
- The following file types are presently unauthorised for download into the network: \*.EXE, \*.MP3, \*.COM and \*.AVI.
- Unauthorised games, mp3 files, AVI files, MPEG files, JPEG files, all kind of compressed files, executable files and all kind of unsupported files will be removed from the Server without previous warning.
- If a user needs for a short period of time a bigger amount of Hard Disk space in the Server or to store unauthorized format files she/he should request authorization from the ICT Department.

### **The importance of the Internet in Education**

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.

*Benefits of using the Internet in education include:*

- *Access to worldwide educational resources including museums and art galleries.*
- *Educational and cultural exchanges between pupils worldwide.*
- *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.*

### **Internet and learning at St Julian's**

- *The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.*
- *Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.*

### **E-mail management**

Much e-mail use is purely of a social nature but,

- *Pupils must immediately tell a teacher if they receive offensive e-mail.*
- *Pupils must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.*
- *Whole-class or group e-mail addresses should be used at Key Stage 2 and below.*

### **The use of Chat Rooms in school's computers.**

- *Pupils are not allowed access to public or unregulated chat rooms.*
- *Children should use only regulated educational chat environments. This use is supervised and the importance of chat room safety emphasised.*
- *Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.*

### **Internet access using St Julian's Computer Network**

- *The school keeps a record of all staff and pupils who are granted Internet access. The record is kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.*
- *At Key Stage 1, access to the Internet is done by adult demonstration with occasional directly supervised access to specific, approved on-line materials.*
- *Parents are informed that pupils will be provided with supervised Internet access.*
- *Secondary students' Parents are asked to sign and return a consent form.*

### **Assessing Internet content**

- *In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school takes 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.*
- *Methods to identify, assess and minimise risks are reviewed regularly.*

### **Filtering Internet content**

- *The school works 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 ICT co-ordinator.*



- *The school manages the configuration of “CensorNet” (an open source filtering software). The filtering strategy is selected to suit the age and curriculum requirements of the pupil.*
- *Senior staff ensures that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.*
- The school, in discussion with the filtering provider, selects filtering strategies where appropriate.



## INTERNET RESTRICTION FORM

Please complete and return this form to your Form Tutor.

Name of pupil \_\_\_\_\_ Form: \_\_\_\_\_

**Parent:** As the parent or legal guardian of the pupil named above, **I do not grant permission** for my son or daughter to use the Internet in St Julian's School Network.

Parent Signature \_\_\_\_\_ Date: \_\_\_ / \_\_\_ / \_\_\_



**Pupil:** I have read the Student Guidelines for Use of the Internet' and agree to observe the restrictions, which are listed. As a member of the school community, I am expected to abide by the School's Rules and understand that these apply also to the use of the Internet.

Pupil Signature \_\_\_\_\_ Date: \_\_\_\_ / \_\_\_\_ / \_\_\_\_