Loreto Convent School

◇

Gibraltar

PUPIL NETWORK POLICY

This policy reflects the ethos of Loreto Convent School and has been compiled and reviewed with the involvement of children, staff and Governors.

Acceptable Use Policy for the IT Network

Applicable to all eligible pupils at Loreto Convent School

Contents

Document Version: v1.1

Date: March 2010

Review: Every 12 months

Document control and amendment record

NOTE: This is a controlled document as are all quality system files on this network.

Any documents appearing in paper form are not controlled and should be checked against the server file version prior to use.

Amendment Record

- October 2017 No amendments – DDC

- January 2021 – new format - PAC

Acceptable Use Policy for the IT Network

1.1 Purpose

The purpose of this policy is to outline the acceptable use of the Loreto Convent School IT network. This policy also applies to any future remote access of the college IT network and the use of ICT systems managed by the school.

Separate acceptable use policies are available for E-mail and the Internet and users of these services are required to adhere to.

Inappropriate use of the school IT network may expose the school to unnecessary risks including virus attacks, compromise of network systems and services, financial and legal issues. The aim of this policy is to protect all end users.

1.2 Eligibility

All eligible pupils will be issued with logon credentials to access the school IT network.

Every user who is issued with a network logon will be asked to sign to acknowledge that they have read, understood and will comply with this policy.

1.3 Acceptable use

Individuals are responsible for their use of the school computer IT network. The school IT network is provided for use by pupils to support their education. Users are expected to respect the property of others, in particular data held on school systems.

Users must take all reasonable precautions to prevent other persons from using their equipment to gain access to internal or external systems to which they have not explicitly been granted access.

Users should be aware that use of the school IT network and the contents of home directories and workgroups is monitored. No expectation of privacy should be taken with regard to any files. In accordance with UK Law, a designated authority may, on behalf of the school, authorise the monitoring of files.

1.4 Unacceptable use

The school, IT network must not be used for any of the following:

• the creation or storage, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material

• the creation or storage of material which is designed or likely to cause annoyance, inconvenience or needless anxiety

• the creation or storage of defamatory material

• the creation or storage of material such that this infringes copyright or the intellectual property rights of another person

• deliberate activities with any of the following characteristics:

  ▪ wasting staff effort or networked resources, including time and the
  ▪ effort of staff involved in the support of the IT systems
  ▪ corrupting or destroying other users' data
  ▪ violating the privacy of other users
  ▪ disrupting the work of other users
  ▪ using ICT facilities in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment)
  ▪ continuing to use an item of networking software or hardware after being requested that use cease because it is causing disruption to the correct functioning of the network
  ▪ other misuse of networked resources as identified by the network administrator, such as the introduction of "viruses"

Users must in no way attempt to gain access to internal or external systems to which they have not been granted access. This includes browsing the network drives without authorisation.

Users must never allow another person to use their logon or use the logon of another person. Users may be held responsible for the actions of, and any consequences of, any other individual using their logon.

Users must not in any way cause any form of damage to the school's computing facilities or any of the accommodation or services associated with them.

Users must not take food or drink into rooms that contain ICT equipment.

Users must not abuse printing resources (see section 1.9).

1.5 Hardware

Do not move computer equipment or rearrange how equipment is plugged in (computers, power supplies, network cabling, modems etc.).

No internal or external devices e.g. peripheral equipment should be added or removed from computer equipment without consulting IT Support.

Use of personal equipment

Users must not connect personal equipment to the school network.

1.6 Software

Software may only be used for the purposes of learning, research and personal educational development or for other purposes as defined in the licensing agreement. Software may only be used on computer equipment covered by that agreement.

Users must not download or install software.

1.7 File management

It is the responsibility of each user to ensure that they regularly delete files that are no longer required. Limits are imposed on the amount of file storage space made available to individual users. These limits are reviewed on a regular basis by school management/IT Support.

IT Support will monitor the size of individual files stored on a network drives (individual home directories and workgroups) as large files, particularly images or audio and video, use up disc space very quickly and can bring the network to a standstill.

Users are not permitted to store any archive (*.zip, *.rar) or executable files (*exe.*.scr or *.com) on the school network. IT Support will perform regular checks for these files and where files or software of this type are found these will be deleted or access to these files will be removed and further action may follow.

1.8 Security

Passwords

Access to the school IT network is controlled by username and password.

Users and/or IT Support may be required to change passwords if IT Support consider there is a possible security risk.

Passwords must not be divulged to third parties and users must take all reasonable precautions to ensure that their password remains confidential. In particular, passwords must never be written down.

New accounts will be set up with a temporary password and will remain disabled until the user contacts IT Support.

If a temporary password is issued for any reason the user must log on and change the password immediately; failure to do so will create a security risk.

Anti-virus

Users must not interfere with the operation of the anti-virus software or change its configuration.

Transferring files

Users needing to transfer files onto the school network from removable media e.g. CD, USB pen stick, floppy drives should contact IT Support.

Alternatively, users who have access to email may transfer files electronically in accordance with section 3.5 of the Acceptable Use Policy for E-mail.

1.9 Printing

All users will be granted access to print in the school's ICT room, computers can be used for monochrome and/or colour printing. Printing must be authorised by a member of teaching staff. No pupil may print unless the print has been checked. Private printing may be charged at 5p per monochrome and 20p per colour print.

The ability to printing may be withdrawn if this is misused. Examples of misuse include:

• wasting resources e.g. wasting paper by printing multiple copies of the same document, wasting toner by printing documents with dark backgrounds

• printing 'junk' i.e. clipart pictures with captions

• printing anything that is deemed to be offensive

• printing large amounts of documents for personal use i.e. not school work

1.10 Termination of accounts

Computing accounts will be terminated when users cease to be a member of the school.

Files will be archived and removed from the network drives. In the event of the pupil transferring to another school arrangements should be made with IT Support for the appropriate files to be transferred.

1.11 Personal/recreational use

The provision of the school IT equipment is primarily intended for the business of Loreto Convent School. Limited personal use is also permitted, provided this does not interfere with learning or the operation of the network and complies with all school Acceptable Use Policies.

1.12 Monitoring

Users should be aware that use of the IT network, including the contents of home directories, virus activity reports and printing logs, are monitored.

Seen by Governing Body: