Loreto Convent School

Gibraltar

PUPIL EMAIL 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 E-mail

Applicable to all eligible pupils at Loreto Convent School

Contents

Document Version: v1

Date: October 2017

Review: Every 12 months

Document control and amendment record

Acceptable Use Policy for E-mail

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

Version Date Detail Author Approval

- October 2017 No amendments – DDC

- January 2021 – new format - PAC

3 Acceptable Use Policy for E-mail

3.1 Purpose

The purpose of this policy is to outline the acceptable use of e-mail by eligible pupils at Loreto Convent School. Access to e-mail is available via the ICT room or Internet through Webmail.

Inappropriate use of e-mail 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.

3.2 Eligibility

Every user who is entitled to an e-mail address will be asked to sign to acknowledge that they have read, understood and will comply with this policy. A signature will also be required from a parent/guardian/carer and access to e-mail will not be granted until this has been received.

3.3 Acceptable use

Loreto Convent School provides an e-mail system to support its activities and access to this system is granted to users on this basis.

Users should be aware of current e-mail etiquette and procedures for dealing with spam/unsolicited mail.

Users should be aware that e-mail use and the contents of e-mail folders is monitored. E-mail messages sent and received from the school e-mail system are not private property; they form part of the administrative records of the school and may be inspected at any time. In accordance with UK Law, a designated authority may, on behalf of the school, authorise the monitoring of communications and or access logs.

3.4 Unacceptable use

Users must not start or forward any chain e-mails, jokes, spam, animations etc. Do not forward any e-mails warning about viruses as they are invariably hoaxes. If in doubt, contact IT Support directly for advice.

Users must not distribute or disseminate any images, text or material which might damage, overload, affect, or have the potential to affect, the performance of the school IT network and/or external communications.

Users must not send or forward any material that could be considered to be obscene, suggestive or defamatory or may harass, distress or otherwise offend the recipient. Users must not send or forward any material which may be considered to be libellous, pornographic, sexually explicit, or which includes hostile material relating to gender, sex, race, sexual orientation, religious or political convictions or disability, or incitement of hatred, violence or any illegal activity. Due regard shall be given to the provisions of the Malicious Communications Act 1988 in addition to school guidance in this respect.

Users who open an e-mail containing any material referred to in the paragraph above should inform IT Support. If the e-mail originated from a sender from outside the school who is personally known to the recipient, it is the responsibility of the recipient to delete the e-mail immediately and contact the sender to request that no messages of similar content are received in the future. Failure to do so may result in e-mail facilities being withdrawn.

Users are not permitted to distribute any files that infringe copyright.

Users must not transmit any viruses or malicious code.

Users must not attempt to access the mailbox of another user.

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

Users must not send e-mails purporting to come from another user by forging the email address of the sender (spoofing).

Users must not disclose their school e-mail address to external organisations, as this information may be passed to other organisations generating unsolicited 'junk' mail.

Users must not use their school e-mail address to sign up to any websites unless authorised and instructed to do so by their teacher.

Excessive use of the e-mail system for 'chatting' to friends will not be allowed.

Any personal use that disrupts learning will not be allowed.

3.5 Attachments (sending & receiving)

Only attachments relating to school work should be sent.

All e-mails sent from or received by the school are scanned for blocked file names and blocked file types by the school's e-mail provider. If the file name or file type of an attachment matches any of the blocked rules then that attachment is replaced with a warning text file and the message is delivered to the recipient. The rules for blocked file names and blocked file types can be obtained by contacting IT Support.

Access to attachments is further restricted by Microsoft Outlook. These restrictions may either deny access to an attachment or prevent users opening the attachment directly from the e-mail (the attachment must be saved before it can be opened). If these restrictions prevent a user from accessing an essential attachment they should contact IT Support.

Attachments must be no bigger than 1Mb in size. This is important, not only to stop the network slowing down but also to ensure that data is transferred efficiently and securely. Files larger than 1Mb can only be sent out by arrangement with IT Support.

Large attachments (over 1Mb) containing homework that need to be sent in to school should be emailed to admin@loreto.gi . The e-mail must clearly state the pupil's name and class to enable the office staff to transfer the file to the correct teacher.

3.6 Viruses

All e-mails sent from or received by the school are scanned by the school's e-mail provider for viruses. If a message is found to contain a virus the message is discarded. Neither the sender nor the recipient is informed since most viruses spoof the sender's address. A copy of the message headers is logged in a database together with the identity of the virus detected. This database is maintained by the school's e-mail provider.

IT Network.

3.7 Mailbox management

Users will be allocated a mailbox of a 2GB capacity. It is the responsibility of each user to ensure that they regularly delete e-mails that are no longer required and to ensure that the Deleted Items folder is emptied. If users fail to manage mailboxes e-mail privileges may be withdrawn.

3.8 Monitoring

No expectation of privacy should be taken with regard to e-mails. Users should be aware that e-mail use, including the contents of e-mail folders, is monitored in accordance with this policy and the school's Policy on Monitoring and Interception.

E-mail messages that have been deleted from the system can be traced and retrieved. Therefore, all persons having a part in creating or forwarding any offending e-mail can be identified. This feature will only be used for monitoring purposes and not for retrieving messages that have been deleted accidentally.

Seen by Governing Body: