Loreto High School Chorlton

Staff Acceptable Use of ICT Policy

Approved: June 2015

Staff Acceptable Use of ICT Policy

This Policy has been written to ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating using ICT with pupils. Members of staff should also make themselves familiar with the school's E-safety Policy and Data Protection Policy. Training in the use of classroom control software can be requested by any staff from the ICT faculty.

1. General

In this policy the term ICT includes a wide range of systems, including the internet, intranet, network storage, mobile phones, PDAs, digital cameras, email and social networking. ICT use may also include personal ICT devices when used for school business.

Staff must ensure that their use of the school ICT is always responsible and professional and does not bring the school's reputation into disrepute. Offensive or illegal material must not be browsed for, viewed, downloaded, uploaded or sent to anyone.

Staff must ensure that their electronic communications with pupils and staff including email, IM and social networking are compatible with a professional role and that messages cannot be misunderstood or misinterpreted.

Staff must notify the Head of ICT if they access an unsuitable website or receive an offensive email.

Copyright and intellectual property rights must always be respected.

2. E-Safety

Staff are responsible for promoting e-safety with students in their care and for helping them to develop a responsible attitude to system use, communications and publishing. Staff should familiarise themselves with the E-Safety Policy.

Staff must report any incidents of concern regarding children's safety to the E-Safety Coordinator, the Designated Child Protection Coordinator or Headteacher.

3. Emails

Email communications can be legally binding, and consequently can be used as evidence of defamation and libel, harassment and of creating or breaking contracts.

They often contain personal data, in the form of facts, intentions or opinions about individuals, and are therefore subject to the Data Protection Act; this includes the right of an individual to request a copy of the data held about them.

Emails must be of a professional standard. It is a good idea to start your email message with a salutation to the addressee, for example Dear John, or Good Morning Mr Smith, as appropriate, to help avoid any confusion if an email is sent mistakenly to the wrong email address.

Staff should be careful when sending emails containing confidential information. Confidential information includes personal information relating to an identifiable individual, that the individual would expect to be treated as private and confidential. Examples might be names of staff and pupils, dates of birth, addresses, national insurance numbers, school marks, medical information, exam results, SEN assessments, religion, sexual orientation, criminal offences, salary and staff development reviews.

Some information, though not relating to individuals, may nonetheless need to be kept confidential. This might include details of the building security, financial and banking information.

When sending confidential emails, staff should consider sending their message and any accompanying additional information in the form of password protected attachments, checking that the email address of the recipient is correct before pressing 'send'. The password will need to be sent separately to the recipient; it may be appropriate to do this in person or by telephone (eg for colleagues in school) or by separate email.

Staff must only use their school email account to send all emails relating to school business.

4. Monitoring

Internet, email and all other ICT use may be monitored and recorded to ensure compliance with school policies, to prevent the spread of computer viruses, to resolve a user problem or to ensure there is no improper or illegal use.

The school may exercise its right to intercept email and to delete inappropriate materials where it believes inappropriate or unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Day to day monitoring is controlled by the Head of ICT.

Any investigation other than day to day monitoring must be authorised by the Head teacher.

5. System and Data Security

Staff must respect system security. Staff should only access the school network with the user name and password they have been allocated. Passwords should be kept secure and must not be disclosed to anyone other than an authorised system manager. Staff must not allow unauthorised individuals to access email, internet or intranet.

Staff must not install any software or hardware onto school ICT equipment without permission from the Head of ICT.

Care must be taken that confidential information is kept secure and used appropriately whether in school, taken off the school premises or accessed remotely. In particular, confidential information relating to human resources matters, child protection and safe guarding issues and individual's contact details must never be stored on staff personal devices.

Staff should ensure that confidential information cannot be viewed on their work screen or desk by unauthorised persons. Screens should be locked or logged off when unattended. Confidential information should be stored securely when not in use.

Electronic documents that include confidential information must be password protected, and the password kept securely. Passwords should be reasonably complex, including a mix of upper and lower case letters, numbers and symbols. They should be kept securely and changed regularly.

Care must be taken not to leave confidential matter on printers and copiers. All printed matter that includes confidential information must be disposed of using the confidential waste bins sited around the school.

Images or data recorded on personal devices such as mobile phones should be transferred to the school network as soon as practicable and deleted from the personal device.

6. Private Use

Staff should note that personal use of the school information systems must be confined to non-teaching time and kept to a minimum. It should not interfere with the proper performance of their duties.

Personal emails should be clearly distinguished from school business emails, for example by marking personal emails as 'personal'.

Staff conduct when using the internet or email system for school business or private use must always be professional and responsible.

Telephone, email and internet must not be used to carry out private commercial activities.

Staff should not store personal files such as music, video, photographs or games on school ICT equipment or network.

7. On Leaving Employment at Loreto High School

All school equipment and data, for example laptops and tablets, mobile phones and USB memory devices, must be returned by the last day of the employment contract. Devices should be returned via the School Business Manager.

Entitlement to access an individual's email account will normally cease on the date of the contract termination.