St Mary's Catholic High School, Leyland

IT Acceptable Use Policy

Created: Nov 2015 **Reviewed: Spring 2018**

Description of Policy

This policy applies to all staff, students and visitors of St Mary's Catholic High School, Leyland and those that use the school's online services remotely.

Scope

The following regulations apply to users of all IT facilities and online services. Staff and students should note the consequences of failing to comply with these regulations, particularly that disciplinary action may be taken by the school for failure of a user to comply with them.

Definitions

Desktop Computers: Static Desktop & Workstation computers owned, leased or hired by the school.

Mobile Devices or Tablet Computers: (such as an iPad)

Portable: hand-held devices owned, leased or hired by the school that provide computing and information storage/retrieval capabilities.

Users: All staff and students of the school and other users who have been given permission to use the school's IT facilities and learning resources.

Facilities: IT facilities located in the school and services which are available online (including the Virtual Learning Environment, Email and any additional services which may be added), including networks, servers, desktop computers and portable computers, mobile devices and tablet computers together with the software and data stored on them. Any IT use carried out on equipment connected to the school network, whether or not this involves the use of a school-based, personal or school-owned computer.

Learning Resources: All learning resources including (but not exclusively) text, video, audio, which are available to the school's users either on the network or the Internet.

Designated Authority: The Designated Authority refers to the school's Governors, Headteacher and Senior Leadership Team (SLT). The Designated Authority may delegate responsibility for particular areas to appropriate school staff.

Relevant Legislation

Users must comply with all UK legislation relating to the use of information, computers and networks. These laws include, but are not limited to:

a) General Data Protection Regulations (GDPR) 2016. This act makes provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

b) Copyright, Designs & Patents Act 1988. Copyright material includes literary works (including computer software), artistic works (including photographs), sound recordings (including music), films (including video) and databases.

c) Computer Misuse Act 1990. The act provides safeguards for computer material against unauthorised access or modification.

d) Privacy and Electronic Communications (EC Directive) Regulations 2003. These regulations prohibit the sending of unsolicited marketing, offensive or threatening Emails, SMS or text messages. In addition, the regulations control the use of cookies.

e) Fraud Act 2006. The Act prohibits 'phishing' whereby official-looking Emails guide unsuspecting users to fake websites (e.g. fake bank websites) in order to steal their login details. Creating or possessing software to enable this activity is also an offence.

Use of IT Resources

The school's IT facilities are provided for educational, administrative, research and personal development use by staff in the course of their employment and by students in the course of their education.

School IT facilities, with the exception of portable computers and mobile devices should not be moved or disconnected without the prior agreement of the Designated Authority.

Members of staff must not contact current St Mary's Catholic High School students via social networking sites or via their own personal email account.. Staff should ensure they conduct their on-line presence in a manner in keeping with their professional status as an employee of the school.

Students are not permitted to use the school's IT facilities for personal use and must not connect any personal device to the school's Wi-Fi network.

Staff must not attempt to contact any student of the school through the use of social networking sites or via their own personal email account.

Students must not attempt to contact any staff member of the school through the use of social networking sites.

Damage

If accidental damage occurs, this must be reported to a senior member of staff. The term 'damage' includes any unauthorised installation of hardware or software. We expect that users will not cause any intentional damage to the school’s IT facilities.

Security

All of the school’s IT facilities have been marked with SmartWater, have anti-virus protection and activity monitoring software installed, including the monitoring of email activity. Users must not deliberately attempt to bypass the proxy server, introduce any virus, worm, Trojan horse or other harmful or nuisance program or file into any IT equipment or take deliberate action to circumvent any precautions taken or prescribed by the school to prevent this. Users must not attempt to penetrate the security and/or privacy of other users' files or attempt to install unauthorised software. Users must not use school IT facilities to access, produce, obtain, download, store, view, share, or distribute material (including images, video, text or sound files) which is either illegal under UK law, in breach of copyright law and/ or can reasonably be judged to be offensive, obscene, indecent, abusive or likely to incite racial hatred.

Passwords

Protecting the school’s computers, systems, data and communications from unauthorized access is of paramount importance; strong passwords play a critical role in this process especially when systems can be accessed remotely. All use of the school’s user accounts, desktop computers, notebook PCs, servers, online services and electronic communications must conform to the following rules both locally and remotely:

Passwords must not be written, e-mailed, shared or otherwise made known to anyone other than the user involved.

No passwords are to be shared in order to “cover” for another individual who is out of school or otherwise indisposed. Instead, contact ICT Services for a temporary account.

No accounts must be shared. Passwords should never be physically written on paper nor written and concealed near a workstation or stored electronically. All passwords must be changed when requested and must never be reused.

Password Complexity

Passwords for all end user systems must meet the following criteria:

At least eight characters in length

Upper case letter (A-Z)

Symbols: !, @, #, $, %, ^, &, *,)

Lower case letter (a-z)

Numbers (0-9)

Passwords must not include:

Any portion of your name

Date of birth

Nickname

Any portion of your address

Username

Family name

Pet name

The word “Password”

Sports team

A name or word that appears in a dictionary

All staff computers must be locked to prevent unauthorised access when unattended.

Remote Access

Remote access is available to all staff members. When a staff member uses their own equipment, they are responsible for the maintenance and repair of it.

Acknowledgment of ICT Acceptable Use Policy

By Logging onto the school’s computer network you indicate your acceptance of the above terms and conditions.