

Policy

ICT Acceptable Use for Staff

Published: December 2011
For Review: 2012–13





Our Purpose

The work of the school is the spiritual, moral, intellectual, aesthetic and physical development of each pupil. It seeks to put Christ at the centre of every activity, worship, learning and service to others.

This plan was adopted by the Governing Body

Signature:

A handwritten signature in black ink, appearing to read 'R Lavery', written over a horizontal line.

Mr R Lavery, Chair of Governing Body

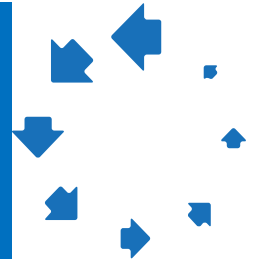
Date:

7/12/2011

St. Mary's Network

ICT Acceptable Use Policy for Staff

Version 2.10



The use of the latest technology is actively encouraged at St. Mary's. With this comes a responsibility to protect users and the school from abuse of the system.

All staff, therefore, must adhere to the policy set out below. This policy covers all computers, laptops and electronic devices within the school, irrespective of who owns the device.

Staff and students are expected to behave responsibly on the school computer network and with the ICT equipment.

1) Access

As a staff member at St Mary's, I have access to the following ICT facilities:

- 1.01 Computers throughout the school campus
- 1.02 Smartboards in all of the teaching rooms
- 1.03 Secure usernames and passwords for logging into:
 - 1.03.1 School computers
 - 1.03.2 The internet
 - 1.03.3 Sims.net (management information system)
 - 1.03.4 Sims Learning Gateway
- 1.04 An accredited, filtered Internet connection from any computer in school
- 1.05 1 GB of My Documents – personal user space on the school network.
- 1.06 Personal 'My Site' user space (and web space) on the school Learning Platform with 500Mb storage.
- 1.07 Access to the school network and the learning platform to store and share learning resources
- 1.08 A personal email account with 500mb of email storage space (accessed through the Learning Platform).
- 1.09 Access to network printers. All staff are given £8.00 in printing funds every month.

- 1.10 Access to resources such as scanners, digital cameras, visualisers and microphones.
- 1.11 Access to the following software for home computer use:
 - 1.11.1 Microsoft Office 2007 (and Microsoft Office 2011 for Apple)
 - 1.11.2 Adobe Master Collection CS5
 - 1.11.3 Smart Notebook 10
- 1.12 Access to the School Management Information Systems as appropriate to roll in school.

2) E-safety

- 2.01 I will ensure that I am aware of e-safety issues affecting staff and students. [Click here](#) to visit our E-Safety site on the Learning Platform
- 2.02 I will regularly remind pupils of key e-safety messages such as 'never give out personal details online'.
- 2.03 I will report any accidental access to inappropriate material to my line manager
- 2.04 I will report any inappropriate web sites on the ICT Helpdesk
- 2.05 I will not communicate with students through social networking sites
- 2.06 I will ensure that any personal social networking accounts that I have are secure
- 2.07 I will be vigilant when asking students to search for images
- 2.08 If a student accesses inappropriate material I will report it following the correct procedures
- 2.09 If I suspect a child protection issue I will report it following the correct procedures.
- 2.10 I will not send anyone my credit card or bank account details without checking that it is a secure site with https at the start of the web address
- 2.11 I will always be myself and will not pretend to be anyone or anything that I am not on the internet.

3) Computer Security

- 3.01 I will use computers with care and leave equipment as I found it. I will not tamper with computer systems or devices (e.g. printers and scanners) and their cabling
- 3.02 If I notice that computer equipment or software is damaged or not working correctly, I will report it on the ICT Helpdesk straight away
- 3.03 I will use the ICT Helpdesk to report ICT related issues whenever possible.
- 3.04 I will never try to bypass security features or systems in place on the network, or try to access resources or a user account that I do not have permission for (hacking).
- 3.05 I will never attempt to install software myself and will request a software change through the ICT helpdesk.
- 3.06 I will always keep my user account credentials secure and not tell them to anyone else.
- 3.07 I understand that my staff logon gives me access to systems and information that students and other staff are not entitled to access and I will not under any circumstances allow anyone else access to a computer under my logon credentials
- 3.08 I will not attempt to go beyond my authorised access. This includes attempting to log on as another person, sending email whilst pretending to be another person or accessing another person's files
- 3.09 I will never leave a computer logged on and unattended for even a short space of time. I will log off or lock the workstation. I understand that failure to do this may result in a breach of the data protection act and leave 'personal data' unprotected
- 3.10 I will not display sensitive information or 'personal data' on a public display or projected image (**eg** smartboard). This includes student data in Sims.net
- 3.11 If I think someone else has obtained my logon details, I will report it to ICT support personnel as soon as possible to get my logon credentials changed
- 3.12 I will never knowingly bring a computer virus, spyware or malware into school.
- 3.13 If I suspect a school computer or a removable storage device that I am using contains a virus, spyware or other malware, I will report this to ICT personnel
- 3.14 I will not attempt to connect to another user's laptop or device while at school. You are not permitted to establish your own computer network
- 3.15 I will not eat or drink whilst using computer equipment

3.16 I will not reply to spam emails as this will result in more spam. Delete all spam emails.

4) Inappropriate Behaviour

- 4.01 I will not store, download or distribute music, video or image files on my personal user space unless they are copyright free media files related to school work
- 4.01 I will not knowingly or recklessly send or post defamatory or malicious information about a person or about school
- 4.02 I will not post or send private information about another person
- 4.03 I understand that bullying of another person either by email, online or via texts will be treated with the highest severity
- 4.04 I will not use the internet for gambling
- 4.05 I will not access material that is profane or obscene, or that encourages illegal acts, violence or discrimination towards other people
- 4.06 If I mistakenly access such material I will inform my line manager immediately or I may be held responsible
- 4.07 I will not attempt to use proxy sites on the internet
- 4.08 I will not take a photo or video of a student or another member of staff without their permission
- 4.09 I will not load photos or videos of other staff and students to websites or social networking sites. I will refer this job to ICT personnel (eg if I wish to put pictures from a trip on the learning platform).

5) Monitoring

- 5.01 I understand that all Internet and email usage will be logged and this information could be made available to my manager on request
- 5.02 I understand that all files and emails on the system are the property of the school. As such, system administrators have the right to access them if required
- 5.03 I will not assume that any email sent on the internet is secure. I will use the school email signature with disclaimer

5.05 I understand that all network access, web browsing and emails on the school systems and laptops are logged and may be routinely monitored on any computer screen without the persons knowledge.

6) Best Practice

- 6.01 I will only use school printing facilities to print school work related materials.
- 6.02 I will only print out work that I need as a paper copy – where possible I will use school systems such as email, the learning platform and shared folders to share information electronically.
- 6.03 I will follow the schools procedure and use the ICT helpdesk for requesting printing funds for myself and my students.
- 6.04 I will report it on the ICT Helpdesk if I believe a printer is not working or out of toner.
- 6.05 I understand that my Leeds Learning Network (LLN) email is a work email address, and as such will be used for Professional purposes.
- 6.06 I will only use the approved, secure LLN email system for any school communication
- 6.07 I will only open attachments or download files from trusted sources
- 6.08 I will not view, download or distribute material that could be considered offensive or pornographic
- 6.09 I will obtain the school digital cameras from the ICT Technician to photograph trips and relevant events (I will not use my own cameras without prior arrangement).
- 6.10 I will pass all photographs taken on to the ICT Technician for storage on the school network (I will not keep images of pupils in my personal user space and will ensure they are on a shared networking area)
- 6.11 I will save work regularly using sensible file names
- 6.12 I will organise my files in a sensible manner and tidy my user space and shared resource areas regularly
- 6.13 I will always back up any work that is not saved onto the school network
- 6.14 I will observe health and safety guidelines when using computer equipment
- 6.15 I will leave my computer and the surrounding area clean and tidy

- 6.16 When I leave school for good, I will ensure that I save any files I wish to take with me as my account will be deleted
- 6.17 I will only empty my recycle bin when I am certain I no longer need the files
- 6.18 I will seek advice from ICT staff before ordering any ICT equipment for my department.
- 6.19 I will not share data protected information (including school images) with third party organisations without seeking advice first
- 6.20 I will use an encrypted storage device (such as the USB drive supplied to me by school) to transfer data protected files between home and school.

7) Other Devices

.....

- 7.01 This acceptable use policy applies to school devices (such as iPads and iPod touches) as well as computers.

8) Sanctions

.....

- 8.01 I understand that failure to comply with this Policy could lead to disciplinary action.