

St Mary's Catholic School
IT Acceptable Use Policy

St Mary's Catholic School

IT Acceptable Use Policy

Contents

1 Introduction	3
2 Computing facilities	3
2.1 Definition	3
2.2 Ownership	3
2.3 Desktop PCs	3
2.4 Portable PCs	4
2.5 Software	4
2.6 Data security	4
2.7 Personal data and the Data Protection Act	4
2.8 Freedom of Information Act	5
2.9 Virus protection	5
2.10 Network access	5
2.11 Further general guidance	5
2.12 Care of equipment	5,
3 Electronic mail	6
3.1 Use and responsibility	6
3.2 Content	6
3.3 Privacy	6
4 Internet usage	7
4.1 Newsgroups	7
4.2 Instant messaging	7
5 Private use, legislation and disciplinary procedures	8
5.1 Private use	8
5.2 Updates to this Policy	8
5.3 Relevant legislation	8
5.4 Disciplinary and relation action	8
Appendix 1: Examples of behaviours which require the use of the St Mary's Catholic School disciplinary policy	9
Appendix 2: Action to be taken in cases of suspected abuse of computers if gross misconduct is suspected	10
Appendix 3: Action to be taken in cases of suspected abuse of computers which does not constitute gross misconduct	11

1 Introduction

1.1 The purpose of this document is to ensure that all users (staff, contractors, secondments, visitors etc.) of St Mary's Catholic School's computing facilities are aware of St Mary's Catholic School's policies relating to their use. Effective and proper use of information technology is fundamental to the successful and efficient running of St Mary's Catholic School. However, misuse of information technology -- in particular misuse of e-mail and access to the Internet -- exposes St Mary's Catholic School to liability and is a drain on time and money. It is critical that all users read and understand this document and make themselves aware of the risks and exposure involved.

1.2 It is the responsibility of all users of St Mary's Catholic School's computing facilities to be aware of and follow all St Mary's Catholic School's IT policies and guidelines and to seek advice in case of doubt. St Mary's Catholic School's IT policies are published in the Staff Handbook.

1.3 This policy may be updated or supplemented by specific standards or procedures to reflect further developments in technology or legislation or other relevant changes.

1.4 St Mary's Catholic School encourages the use of the School's computing facilities for the mutual benefit of St Mary's Catholic School and its staff. Similarly the regulations that constitute this policy seek to provide for the mutual protection of St Mary's Catholic School and the rights of its staff.

2 Computing facilities

Access to the School's computing facilities is managed by the ICT manager. Use of any of St Mary's Catholic School's computing facilities is at the discretion of the Headteacher.

2.1 Definition

The phrase 'Computing Facilities' as used in this policy shall be interpreted as including any computer hardware or software owned or operated by St Mary's Catholic School and any allocation of time, memory, disk space or other measure of space on any of St Mary's Catholic School's hardware, software or networks

2.2 Ownership

Computing facilities owned by St Mary's Catholic School and software and/or data developed or created (for whatever reason) on that equipment remains in all respects the property of St Mary's Catholic School. The Patents Act 1977 and the Copyright, Designs and Patents Act 1988 provide for the Intellectual Property Rights (IPR) in that work created by a member of staff in the course of his/her employment is vested automatically to the employer.

2.3 Desktop PCs

Desktop PCs are a critical asset to St Mary's Catholic School and must be managed carefully to maintain security, data integrity and efficiency. Users must consult the ICT manager before installing non-standard software on computers managed by the ICT manager as a Desktop PC. For clarification of a machine's status as a 'Desktop PC' please consult the ICT manager. Non-standard software shall be interpreted as any software that does not comply with the regulation of sub-section 2.5 below. All users have access to appropriate areas on St Mary's Catholic School's file servers for the secure storage of valuable files. Valued documents and files should not be stored on the "C:\\" drive of Desktop PCs. Files stored on the "C:\\" drive of Desktop PCs are at risk of loss through hardware/software failure or automated administrative activity. Desktop PCs include the CPU/hard-drive unit and monitor both of which are asseted components and further, are subject to change control. Users must contact the ICT manager in order to perform a 'swap' of these assets.

2.4 Portable/Laptop PCs

Portable/Laptop PCs are at high risk from loss or theft and require additional security protection. All reasonable precautions must be taken to ensure that hardware is stored securely. Also, to protect the integrity of St Mary's Catholic School systems and data procedures, passwords or authentication devices for gaining remote access to St Mary's Catholic School systems must not be stored with the computer. This includes the saving of passwords into remote access software. Highly confidential data can be encrypted to protect it in the event of Portable/Laptop PC loss. The ICT manager can help with this process. If your Portable/Laptop PC is lost or stolen the ICT manager must be notified as soon as possible and a report made to the police.

2.5 Software

Only software properly purchased and/or approved by the ICT manager may be used on the School's hardware. Non-standard or unauthorised software can cause problems with the stability of computing hardware and it is necessary to contact the ICT manager before the installation of such software. Software or shareware may be downloaded from the Internet or loaded from other sources (e.g. CDROM) when necessary, however it is the responsibility of the individual to ensure that any licensing issues are addressed promptly, either by on-line registration or the purchasing of a valid licence through the ICT manager. In order to comply with our registration with the 'Federation Against Software Theft' the ICT manager must be notified when such additional/new software is installed. The use or copying of software without the licensor's permission is illegal and equally the terms and conditions of software licences must always be adhered to. Whilst it is the user's responsibility to take reasonable care over the configuration of their computer hardware, it is possible for software to be installed on a machine without the full comprehension of the user. Users discovering software that has been installed in an unsolicited manner and which contravenes the licensing regulations above are encouraged to contact the ICT manager who will be happy to assist in resolving any issues.

2.6 Data security and management

You must only access information held on St Mary's Catholic School's computer systems if you have been properly authorised to do so and you need the information to carry out your work. Under no circumstances should you disclose personal or other confidential information held on computer to unauthorised persons. The unauthorised access to and/or unauthorised modification of data is a criminal offence under the Computers' Misuse Act 1990. It is the School's policy to store data on a network drive where it is regularly backed up. You must ensure that data that is not stored on the network file server is regularly backed up. All users should seek to delete unnecessary files and tidy documents and email in-boxes in order to conserve disk space.

2.7 Personal data and the Data Protection Act

St Mary's Catholic School maintains a notification to the Data Protection Commission in compliance with the Data Protection Act 1998. This notification is held on a public register and contains details of the organisations holding and processing of personal data. The Data Protection Compliance officer (the School Bursar) must be informed of all collections of personal data through the annual audit. It is the responsibility of all St Mary's Catholic School staff to ensure that personal data is held and processed within the terms of St Mary's Catholic School's notification and in compliance with the data protection principles.

Personal data shall be:

- . obtained and processed fairly and lawfully
- . held for specified lawful purpose(s)
- . not used or disclosed in a way incompatible with the purpose(s)
- . adequate, relevant and not excessive for the purpose(s)
- . accurate and up to date
- . not kept longer than necessary

- . available to the data subject
- . kept secure.

Staff should note that all data and correspondence, including e-mail messages, held by St Mary's Catholic School may be provided to a data subject, internal or external, in the event of a subject access request.

Procedures for using and storing digital images safely in school

1. Consider using group photos rather than photos of individual children.
2. Ensure that the image file is appropriately named – do not use pupils' names in file names.
3. Ensure that images are appropriately stored and secured on the school's network (on Staff Resources>School Photographs) rather than on your PCs hard drive.
4. Only use images of pupils in suitable dress to reduce the risk of inappropriate use.

2.8 Freedom of Information Act

St Mary's Catholic School is subject to the provisions of the Freedom of Information Act (2000) which provides for the general right of access to information held by public authorities. While St Mary's Catholic School is in the process of meeting the requirements of the Act, staff should be aware that the Act effectively extends rights available under the Data Protection Act to include all types of information held, whether personal or non-personal. Therefore, such data or correspondence may be provided to an applicant in the event of an access request. Further information about this Act may be obtained from the Bursar.

2.9 Virus protection

Anti-virus software is loaded on all computers as standard and is updated regularly via the network. Anti-virus software must not be de-installed or deactivated. Files received by or sent by e-mail are checked for viruses automatically. Remote users are responsible for maintaining up to date virus definitions on their computers and can contact the ICT manager for help as required. Users must not intentionally access or transmit computer viruses or similar software. Non-St Mary's Catholic School software or data files intended to be run on the School's equipment by external people such as engineers or trainers must be checked for viruses before use. If you suspect that a virus has infected a computer then stop using the computer and contact the ICT manager immediately.

2.10 Network access

Passwords protect St Mary's Catholic School systems from access by unauthorised people: they protect your work and the School's information. Therefore never give your network password to anyone else. Procedures are to be put in place on systems to ensure users change passwords on a regular basis, passwords are of a minimum length and old passwords cannot be reused immediately.

Passwords must be six or more characters long and include at least one numeric or non-alphabetic special character.

St Mary's Catholic School does not allow the connection of non-School computer equipment to the network without prior written request and technical approval. This includes connection via dialup or Virtual Private Networking (VPN). Only the ICT manager or headteacher can give authorisation for a wireless network point to be installed.

2.11 Further general guidance

St Mary's Catholic School users must ensure prior approval through the Leadership Group to:

- set-up world wide web sites on St Mary's Catholic School computing facilities
- publish pages on external world wide web sites containing information relating to St Mary's Catholic School
- enter into agreements on behalf of themselves or St Mary's Catholic School via a network or electronic system

- transmit unsolicited commercial or advertising material to other users of a network or to other organisations
- be used for external business interests or personal gain

2.12 Care of Equipment

All users must take appropriate and reasonable care with ICT equipment. It should be left in a clean and usable condition by the user. Misuse or carelessness can lead to appropriate disciplinary procedures. Equipment must not be moved from one department or location to another without the ICT manager receiving written confirmation.

3 Electronic mail

3.1 Use and responsibility

St Mary's Catholic School's electronic mail (e-mail) system is provided for the School's business purposes. E-mail is now a critical business tool but inappropriate use can expose St Mary's Catholic School and the user to significant liability. Liability can arise in a number of ways including, among others, copyright or trademark infringement, misuse of confidential information, defamation and liability for inaccurate statements.

The e-mail system costs the School time and money, it must be used judiciously in the same manner as other School resources such as telephones and photocopying. School-wide e-mail messages must be business related and of significant importance to all staff.

3.2 Content

E-mail messages must be treated like any other formal written communication.

E-mail messages cannot be considered to be private, secure or temporary.

Email can be copied and forwarded to numerous recipients quickly and easily and you should assume that they could be read by anyone.

Improper statements in e-mail can give rise to personal liability and liability for St Mary's Catholic School and can constitute a serious disciplinary matter. E-mails that embarrass misrepresent or convey an unjust or unfavourable impression of St Mary's Catholic School or its business affairs, staff, suppliers, customers or competitors are not permitted.

Do not create or send e-mail messages that are defamatory. Defamatory e-mails whether internal or external can constitute a published libel and are actionable.

Never send confidential or sensitive information via e-mail. E-mail messages, however confidential or damaging, may have to be disclosed in court proceedings.

Do not create or send e-mail messages that may be intimidating, hostile or offensive on the basis of sex, race, colour, religion, national origin, sexual orientation or disability.

It is never permissible to subject another member of staff to public humiliation or ridicule; this is equally true via e-mail.

Copyright law applies to e-mail. Do not use e-mail to transmit or circulate copyrighted materials.

3.3 Privacy

E-mail messages to or from you cannot be considered to be private or confidential. Although it is not policy to routinely examine the content of individuals' e-mail, St Mary's Catholic School reserves the right to monitor messages, at any time, for specific instances in which there is good cause for such monitoring or some legal obligation to do so. Good cause shall include the need to fulfil the School's obligations, detect staff wrongdoing, protect the rights or property of the School, protect IT system security or to comply with legal process.

Messages sent or received may be copied and disclosed by the School for lawful purposes without prior notice.

It is not permissible to access or to send e-mail from another member of staff's personal account either directly or indirectly, unless you obtain that person's prior written approval.

4 Internet usage

The laws of all nation states regulating such diverse subjects as intellectual property, fraud, defamation, pornography, insurance, banking, financial services and tax apply equally to on-line activities. However, the practical legal position regarding Internet usage is often uncertain.

Strictly, documents must not be published on the web which are defamatory or which may constitute intimidating, hostile or offensive material on the basis of sex, race, colour, religion, national origin, sexual orientation or disability under the sovereign law of the country in which the web server hosting the published material is sited.

Strictly, material must not be accessed from the web which would be objectionable on the above grounds under the sovereign law of the countries in which the networks transporting the material are sited or which would violate the Acceptable Use Policies of those networks.

Given the impracticality of assessing the exact legal position with regard to the previous two paragraphs, St Mary's Catholic School's Acceptable Use Policy governing material that could be objectionable on the above grounds is grounded in English law, on which basis it is reasonable to expect St Mary's Catholic School staff to have good awareness and to be able to exercise good judgement. If in doubt over a specific case please escalate through your Subject Leader/Line Manager.

Once information is published on the worldwide web anyone from anywhere in the world can access it. It is therefore critical that material of a proprietary or sensitive nature should not be published on unsecured public web sites. All Internet usage from the St Mary's Catholic School network is monitored and logged. Reporting on aggregate usage is performed on a regular basis. When specific circumstances of abuse warrant it, individual web sessions will be investigated and linked to the relevant staff user account. Such an investigation may result in action via St Mary's Catholic School's Disciplinary Procedure and possibly criminal investigation.

Copyrights and licensing conditions must be observed when downloading software and fixes from the web sites of authorised software suppliers. Files so protected must never be transmitted or redistributed to third parties without the express permission of the copyright owner.

4.1 Newsgroups

Postings to newsgroups are in effect e-mails published to the world at large and are subject to the same regulations governing email as above. Always include a disclaimer with a posting if it could be interpreted as an official statement or policy of St Mary's Catholic School. For example:
"The views expressed are my own and do not necessarily represent the views or policy of my employer."

4.2 Instant messaging

Instant messaging is free, fast, real-time and powerful. However instant messaging also carries inherent risks: lack of encryption (allowing the possibility of eavesdropping) logging of chat conversations without a user's knowledge and virus risks. Due to these risks, St Mary's Catholic School does not currently allow the use of instant messaging for the communication of sensitive or proprietary School information.

5 Private use, legislation and disciplinary procedures

5.1 Private use

Computing facilities are provided for St Mary's Catholic School's business purposes and responsible personal use is allowed provided there is no conflict with the interests or requirements of St Mary's Catholic School. St Mary's Catholic School does not accept liability for any personal loss or damage incurred through using the School's computing facilities for private use.

5.2 Updates to this Policy

In the light of changes in the business, technology, legislation or relevant standards it may be necessary to update this policy from time to time. Notification to all staff will be made when updates are available.

5.3 Relevant legislation

The following is a list of Acts that apply to the use of St Mary's Catholic School computing facilities:

- . Regulation of Investigatory Powers Act 2000
- . Computers' Misuse Act 1990
- . Protection from Harassment Act 1997
- . Sex Discrimination Act 1975
- . Race Relations Act 1976
- . Disability Discrimination Act 1995
- . Obscene Publications Act 1959
- . Telecommunications Act 1984
- . Protection of Children Act 1978
- . Criminal Justice Act 1988
- . Data Protection Act 1998
- . The Patents Act 1977
- . Copyright, Designs and Patents Act 1988
- . Defamation Act 1996
- . Freedom of Information Act 2000
- . Human Rights Act 1998

5.4 Disciplinary and related action

As the Government's lead Agency on the use ICT in education, St Mary's Catholic School wishes to promote the highest standards in relation to good practice and security in the use of information technology. Consequently it expects and supports the integrity of its staff. In exceptional circumstances, where there are reasonable grounds to suspect that a member of staff has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow.

Appendix 1 details examples of behaviours which are unacceptable within St Mary's Catholic School and provides examples of behaviour deemed as Gross Misconduct and Misconduct.

Appendix 2 provides a Flowchart of action to be taken in cases of suspected abuse of computers that constitute Gross Misconduct.

Appendix 3 provides a Flowchart of action to be taken in cases of suspected abuse of computers that constitute Misconduct.

Reviewed: 2 December 2008

Review Date: July 2009

Responsible Governor Committee: Personnel

Appendix 1: Examples of behaviours which require the use of the St Mary's Catholic School disciplinary policy

(A) GROSS MISCONDUCT

Examples:

1. Criminal Acts – for example in relation to child pornography.
2. Visiting pornographic sites (adult top shelf materials) except where this forms an authorised part of the staff member's job (for example 'Testing'). Harassment – inappropriate e-mails or printed e-mails sent to a colleague, even if sent as a joke. Harassment can take a number of forms and is defined as unwanted conduct that affects the dignity of people within the workplace.
3. Obscene racist jokes or remarks which have been shared internally and externally – reflects on the image of employer and brings the organisation into disrepute.
4. Downloading and installation of unlicensed products.
5. Viewing sexually explicit materials, except where this forms an authorised part of the staff member's job (for example 'Gridwatch').
6. Chat rooms – sexual discourse, arrangements for sexual activity.
7. Violation of St Mary's Catholic School's registration with the Federation Against Software Theft – such as software media counterfeiting or illegitimate distribution of copied software.

(B) MISCONDUCT

Examples.

1. Frivolous use of the School's computing facilities that risk bringing St Mary's Catholic School into disrepute. The distribution of animated Christmas card programmes or 'chain e-mails' beyond the internal e-mail system would represent examples of such misconduct.
2. Entering into contracts via the Internet that misrepresent St Mary's Catholic School. Contracts are legally binding agreements and a member of staff must not enter into any agreements via the Internet to procure goods or services where St Mary's Catholic School is liable for this contract, without first consulting St Mary's Catholic School's Financial procedures (available from the Finance Office).
3. Deliberate introduction of viruses to systems.

This list is not exhaustive, but sets the framework of St Mary's Catholic School's approach to misuse of computing systems.

St Mary's Catholic School has the right to monitor staff usage of computer equipment where there is evidence to suggest misuse. (Regulation of Investigatory Powers Act 2000).

Appendix 2: Action to be taken in cases of suspected abuse of computers if gross misconduct is suspected

Where a manager suspects misuse

Or

Where a member of staff has concerns about a colleague → and discusses with line manager or if this would compromise the situation, reports to the next level of management

Referral to
Headteacher
(for information)



Discussion with Assistant Headteacher
or Bursar



Referral to
Headteacher
(for information)



Contact the ICT manager to provide data on the individual's use of computer.



The ICT manager will make a judgement based on information available as to whether investigation is necessary and will discuss evidence with Assistant Headteacher &/or Bursar. If yes, agree to nominate Investigating Officer who will:



Discreetly stop the member of staff from using the computer further. Ask the member of staff to attend a private area with a friend or colleague in attendance.



Suspension Interview

The Investigating Officer will give brief details of what is suspected and suspend the member of staff from work to allow further investigation. Suspension will be on full pay. The member of staff will be escorted from the premises and told to refrain from work until further notice. They will not be allowed to attend the premises until asked to do so by management and will be excluded from using any equipment or property of St Mary's Catholic School.



Decision to advise the Police for criminal investigation

On the facts that are immediately available, a decision will be taken whether to refer the matter to the Police for criminal investigation. This does not preclude the matter being referred to the Police at any later stage when a formal investigation has been undertaken within the disciplinary procedure.



St Mary's Catholic School Disciplinary Procedure

The Investigating Officer will then continue a formal investigation and the St Mary's Catholic School disciplinary Policy will be adhered to.

Appendix 3: Action to be taken in cases of suspected abuse of computers which does not constitute gross misconduct

Where a manager suspects misuse

Or

Where a member of staff has concerns about a colleague and discusses the situation with their manager or if this would compromise the situation, reports to the next level of manager



Discussion with headteacher



Contact with ICT Manager to provide data on the individual's use of computer



The headteacher will make a judgement based on information available as to whether investigation is necessary and will discuss evidence Personnel. If yes, agree to nominate Investigating Officer who will:



Investigate by asking the member of staff for an explanation and make other enquiries and investigate as required.



At the conclusion of the investigation if there are reasonable grounds to conclude that a criminal act has taken place



Advise Chair of Governors for information



A decision to enter the Gross Misconduct Investigation Procedure described in Appendix 2, which would require suspension of the member of staff

Or Make a judgement that a verbal warning is needed

Or Enter the Disciplinary Process and convene a Disciplinary Hearing

Or Decide there is no case to answer and the matter concludes

END