St Charbel’s College
142 Highclere Avenue
Punchbowl

IT USER POLICY
2007

CONTENT

Acceptable use of Information Technology (IT) facilities
Guidelines for staff
Guidelines for students
Appendix A
<table>
<thead>
<tr>
<th>CONTENT</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceptable use of Information Technology (IT) Facilities</td>
<td>4</td>
</tr>
<tr>
<td>1. Overview</td>
<td>5</td>
</tr>
<tr>
<td>2. Scope</td>
<td>5</td>
</tr>
<tr>
<td>3. Users with Authorised Accounts</td>
<td>5</td>
</tr>
<tr>
<td>4. Other Users</td>
<td>6</td>
</tr>
<tr>
<td>5 Acceptable Usage of College IT Facilities</td>
<td>6</td>
</tr>
<tr>
<td>6. User Accounts and Passwords</td>
<td>8</td>
</tr>
<tr>
<td>7. College Responsibility</td>
<td>8</td>
</tr>
<tr>
<td>8. Monitoring Use</td>
<td>9</td>
</tr>
<tr>
<td>9. Compliance</td>
<td>9</td>
</tr>
<tr>
<td>10. Exceptions</td>
<td>10</td>
</tr>
<tr>
<td>11. Implementation and Review</td>
<td>10</td>
</tr>
<tr>
<td>12. Communication</td>
<td>10</td>
</tr>
</tbody>
</table>

| Guidelines for Staff on Use of IT Facilities, Including Email and the Internet | 11 |
| 1. Responsibilities of Staff | 12 |
| 1.1 Acceptable Use of IT Facilities | 12 |
| 1.2 Copyright Law | 13 |
| 1.3 Honesty in Representation and Identity | 15 |
| 1.4 Security | 16 |
| 1.5 Non Interference | 17 |
| 2. Unacceptable or Prohibited Use of IT Facilities | 17 |
| 2.1 Purpose | 17 |
| 2.2 Examples of Unacceptable Use | 18 |
| 2.3 Inadvertent Unacceptable Use | 19 |
| 2.4 Seeking Advice on Use | 19 |
| 2.5 Use for Personal Purposes | 19 |
| 2.6 What to do When Misuse is Observed | 19 |
| 2.7 What Happens Following a Report of Alleged Misuse | 20 |
| 2.8 Penalties for Misuse of IT Facilities | 21 |
| 3. Privacy | 21 |
| 3.1 Privacy Limitations | 21 |
| 3.2 Privacy Legislation | 22 |
| 3.3 Freedom of Information | 22 |
| 4. Monitoring of Use of IT Facilities | 23 |
| 4.1 Routine Monitoring | 23 |
| 4.2 Other Monitoring | 24 |
| 5. Email Bulletins and Distribution Lists | 24 |
| 5.1 General Notices | 24 |
5.2 All staff Notices and All Student Notices ................................................. 24
6. Other Information .......................................................................................... 24
6.1 Charging for Internet Use ......................................................................... 24
6.2 How to Reduce the Cost of Internet Use .................................................. 25
6.3 Procedures Relating to Email When a Staff Member Leaves ................. 26

Guidelines for Students on Use of IT Facilities, Including Email and the Internet

1. Responsibilities of Students ............................................................................ 27
   1.1 Acceptable Use of IT Facilities ................................................................. 27
   1.2 Copyright Law ........................................................................................... 28
   1.3 Honesty in Representation and Identity .................................................. 29
   1.4 Security ..................................................................................................... 30
   1.5 Non Interference ....................................................................................... 30
2. Unacceptable or Prohibited Use of IT Facilities ............................................. 31
   2.1 Purpose ...................................................................................................... 31
   2.2 Examples of Unacceptable Use ................................................................. 31
   2.3 Inadvertent Inappropriate Use ................................................................ 32
   2.4 Seeking Advice on Use ............................................................................. 32
   2.5 What to do When Misuse is Observed ..................................................... 32
   2.6 What Happens Following a Report of Alleged Misuse ............................ 32
   2.7 Penalties for Misuse of IT Facilities ......................................................... 33
3. Privacy ............................................................................................................ 33
   3.1 Privacy Limitations ................................................................................... 33
   3.2 Freedom of Information ........................................................................... 34
4. Monitoring Use of IT Facilities ...................................................................... 34
   4.1 Routine Monitoring .................................................................................. 34
   4.2 Other Monitoring ..................................................................................... 35

Appendix A ...................................................................................................... 36
1. Associated Documents ................................................................................ 36
2. Relevant Legislation ..................................................................................... 36
3. Relevant Terms ........................................................................................... 36
Acceptable Use of Information Technology (IT) Facilities

Date of Authorisation: Wednesday, 2 May 2007

Effective Date: Wednesday, 2 May 2007

Date of Last Amendment: Wednesday, 2 May 2007

Reference Authority: Principal

Related documents: This Policy must be read in conjunction with the documents listed in Appendix A. Those documents address specific implementation issues such as Internet use, email and privileged access to systems.

Contact Person: Any person who requires assistance in understanding any aspect of this document should contact the College's Network Administrator (sanjeeva.jayasuriya@stcharbel.nsw.edu.au).
1. Overview

St Charbel’s College provides Information Technology facilities (IT facilities) to support its teaching and learning, research, administrative and business activities. IT facilities includes all computing and communication equipment, software, services, data and dedicated building space used in connection with information technology, which is owned by, leased by or used under license or agreement by St Charbel’s College. St Charbel’s College recognises its responsibility to ensure the appropriate use of its IT facilities and that it must be protected from damage or liability resulting from the unlawful or inappropriate use of its IT facilities.

2. Scope

This Policy applies to users with authorised accounts (as defined below) to access St Charbel’s College's IT facilities.

3. Users with Authorised Accounts

3.1 It is a requirement that every person who accesses College IT facilities must have an authorised user account for their exclusive use.

3.2 Authorised accounts will only be issued to staff employed by St Charbel’s College, currently enrolled students, visiting academics, contractors or consultants engaged by St Charbel’s College, or other recognised affiliates of St Charbel’s College. In addition, access to particular systems and types of use may require authorisation by the relevant Unit Director/Manager, Faculty Coordinator, Head of School or Principal.

3.3 All users with an authorised account must comply with this policy when using St Charbel’s College's IT facilities.
4. Other Users

4.1 This policy recognises that some College IT facilities are provided for the use of members of the general public who do not have any formal relationship with St Charbel’s College. Examples of such facilities are College websites that are not subject to some form of access control.

4.2 These users will not be issued with user accounts, and will only be subject to sections 5.1, 5.3 and 5.2 of this policy. In addition, their use of College IT facilities must comply with State and Commonwealth laws and any additional Guidelines issued by St Charbel’s College in relation to their use of the facilities.

5 Acceptable Usage of College IT Facilities

5.1 IT facilities are provided to support St Charbel’s College's teaching and learning, research, administrative and business activities.

5.2 IT facilities are not provided for recreational or personal use unless specifically stated otherwise in the guidelines listed in Appendix A.

5.3 Users of College IT facilities must comply with St Charbel’s College's requirements for acceptable use. *Specific activities that constitute unacceptable use include but are not limited to:*

5.3.1 Deliberate, unauthorised corruption or destruction of IT facilities (including deliberate introduction or propagation of computer viruses).

5.3.2 Deliberate, unauthorised access to IT facilities.

5.3.3 Unauthorised use of data or information obtained from the use of IT facilities.

5.3.4 Use of IT facilities to access, create, transmit or solicit material which is obscene, defamatory, discriminatory in nature, or likely to cause distress to some individuals or cultures, where such material is not a legitimate part of teaching and learning or research (if the material is a legitimate part of teaching and learning or research, an appropriate warning should be given).
5.3.5 Transmission or use of material which infringes copyright held by another person or St Charbel’s College.

5.3.6 Violation of software licensing agreements.

5.3.7 Use of IT facilities to transmit unsolicited commercial or advertising material.

5.3.8 Deliberate impersonation of another individual by the use of their login credentials, email address or other means.

5.3.9 Violation of the privacy of personal information relating to other individuals.

5.3.10 Unauthorised disclosure of confidential information.

5.3.11 Use of IT facilities to harass or threaten other individuals.

5.3.12 Unauthorised attempts to identify or exploit weaknesses in IT facilities.

5.3.13 Unauthorised attempts to make College IT facilities unavailable.

5.3.14 Use of College IT facilities to gain unauthorised access to third party IT facilities.

5.3.15 Use of College IT facilities in unauthorised attempts to make third party IT facilities unavailable.

5.3.16 Use which deliberately and significantly degrades the performance of IT facilities for other users (including the downloading of MP3 files not related to teaching and learning and research).

5.4 Users must also comply with St Charbel’s College's other policies and procedures and other Guidelines as released by Network Administrators.

5.5 If any unacceptable use of College IT systems is detected, it must be reported to the Network Administrator.
5.6 Behaviour which breaches this policy may also breach Commonwealth and State law.

6. User Accounts and Passwords

6.1 All user accounts must have one person nominated as the person responsible for that account.

6.2 Users are responsible for all activity initiated from their accounts, unless it is established that the activity was done by another person who gained access to the user's account through no fault of the user.

6.3 Users must select passwords that cannot be easily guessed and they must not divulge passwords to others, including other staff and students.

6.4 Users must not attempt to determine another user's password.

6.5 If the security of a password is compromised, it must be changed immediately.

6.6 Users are not permitted to authorise others to login using their account.

6.7 Passwords should be changed regularly.

6.8 Users are prohibited from using another user's account.

7. College Responsibility

St Charbel’s College will take reasonable steps to protect its IT facilities from unauthorised and unacceptable use.
8. Monitoring Use

St Charbel’s College reserves the right to monitor any and all aspects of its IT facilities to determine if a user is acting unlawfully or violating this Policy, the associated documents listed in Appendix A, or any other College policy or rule. Such monitoring may include, but is not limited to, individual login sessions, the Internet sites visited by users and the content of electronic communications. Monitoring may be done with or without prior notice to the user. Procedures relating to monitoring use are listed in Appendix A.

9. Compliance

9.1 Users of College IT facilities are responsible for adhering to the provisions of this Policy.

9.2 St Charbel’s College may take remedial action and suspend user access with or without prior notice in response to suspected breaches of this policy.

9.3 Breaches by staff or students that constitute misconduct will be addressed by the relevant staff or student disciplinary procedures. See Appendix A.

9.4 Sanctions for failing to comply with this Policy or the associated documents listed in Appendix A may include:

9.4.1 Immediate withdrawal of access to IT facilities, with or without prior notice.

9.4.2 Action taken under St Charbel’s College’s relevant performance management scheme and/or disciplinary procedures for staff or for students.

9.4.3 Criminal or other penalties imposed by State or Commonwealth legislation.

9.4.4 Financial compensation sought by St Charbel’s College.
10. Exceptions

Requests for exceptions to this policy must be authorised by the Network Administrator and/or Principal. Such requests must be made in writing and will be evaluated based on the case presented to support it.

11. Implementation and review

11.1 All college staff will be responsible for the implementation of this Policy in their respective areas of responsibility.

11.2 The Network Administrator is responsible for regularly reviewing this Policy.

11.3 The Network Administrator has authority to issue from time to time the Guidelines referred to in Appendix A due to changes in the law or changes in the practices of St Charbel’s College.

11.4 The Network Administrator has authority to amend Appendix A and any Guidelines issued with the approval of the Principal.

11.5 Both the Guidelines referred to in Appendix A and any additional Guidelines are afforded the status of Policy.

12. Communication

12.1 Student and Academic Services and the Human Resources Unit are responsible for ensuring that all students and all staff members have access to this Policy through St Charbel’s College website.

12.2 This Policy will be included in the information package provided to all new members of staff.
**Guidelines for Staff** on Use of IT Facilities, Including Email and the Internet

*For the purposes of this policy, the term “staff” includes all teachers (permanent, part-time and casual) and all support staff.

These guidelines provide clarification for staff on the practical application of the College's Policy on Acceptable Use of IT Facilities and they should be read in conjunction with it.

IT facilities includes all computing and communication equipment, software, services, data and dedicated building space used in connection with information technology, which is owned by, leased by or used under license or agreement by St Charbel’s College.

1. Responsibilities of staff
2. Unacceptable or prohibited use of IT facilities
3. Privacy
4. Monitoring use of IT facilities
5. Email bulletins and distribution lists
6. Other information
1. Responsibilities of staff

The following sections set out requirements that are particularly significant and provide relevant information about some of the legislation that governs the use of IT facilities. All staff who uses College IT facilities must comply with the policy, legislation and principles that are referred to here as well as to other directives from the Network Administrator that may be issued.

1.1 Acceptable Use of IT facilities

Information technology facilities may be used only as set out in the Policy on Acceptable Use of IT Facilities.

Staff members must not use IT facilities for the purpose of personal profit making or for commercial activities other than those of St Charbel’s College. Staff use of College IT facilities including email and the internet is conditional upon compliance with all College policies procedures and guidelines, including the Sexual Harassment Policy, Grievance Procedures (Conflict Resolution) and Equal Opportunity Policy as well as with State and Commonwealth laws.

A list of relevant documents and Government legislation with which staff must comply is set out in Appendix A of the Policy on Acceptable Use of IT Facilities.
1.2 Copyright Law

Copyright law restricts the copying of software and other material subject to copyright (documents, music, broadcasts, videos etc) except with the express permission of the copyright owner.

Material, including images and text, are protected by the Copyright Act of Australia. There is no general right for users of copyright material to make digital copies of copyright material. If you wish to load copyright material onto any WebPages specific permission will need to be sought from the copyright owner. Authors of works are granted copyright protection in Australia as soon as the material expression has been created; there is no legal requirement to register the work.

If the work is created in the course of your employment then the employer will own the copyright.

*St Charbel’s College accepts that in accessing these pages:*

1. You may retrieve material for information only.

2. You may save or download a local copy for personal use.

3. You may send it to your printer for personal use or to communicate the information to authorised and potential users, but you may not make any charge for such use.

4. Any commercial exploitation is expressly prohibited.

5. You must clearly acknowledge the source by including the copyright notice in any copy you make.

6. You may not make any modification to the material without the express permission of St Charbel’s College.
1.2.1 Software

Staff may not make use of, or copy, software contrary to the provisions of any agreement entered into by St Charbel’s College. The onus is on staff to consult with Network Administrator to clarify the permitted terms of use if they wish to use any software for purposes other than those for which St Charbel’s College has a license.

1.2.2 Multiple Users

Copies of software used in a multi-access or network environment to allow simultaneous access by more than one user can only be provided if specifically permitted in the contract or software license, or if a copy of the software has been purchased for every simultaneous user.

1.2.3 Email and Copyright

The copyright of an email message is owned by the sender, or the sender's employer. Copyright owners have a variety of rights, including the right to reproduce their work and the right of communication to the public. Forwarding something to an email discussion list would be construed as "to the public". Consider the expectations of the originator; did that person set any conditions on the further communication of their email, or expect that it would not be forwarded to anyone else, or would not be forwarded to a particular recipient.

1.2.4 Spam Act 2003

All email messages sent from a College email account must comply with the Spam Act 2003. This Act sets up a scheme for regulating commercial email and other types of commercial electronic messages. The Spam Act refers to spam as unsolicited commercial electronic messaging. Electronic messaging includes emails, instant messaging, SMS and other mobile phone messaging. A single message may be spam. The message does not need to be sent in bulk, or received in bulk.
There are a large number of commercial electronic messages that can be sent legitimately. They are only considered to be spam if they are sent without the prior consent of the recipient - as unsolicited messages. The rules for sending commercial electronic messages are:

1. Unsolicited commercial electronic messages must not be sent.
2. Commercial electronic messages must include information about the individual or organisation that authorised the sending of the message.
3. Commercial electronic messages must contain a functional unsubscribe facility.
4. Address-harvesting software must not be supplied, acquired or used.
5. Electronic address list produced using address-harvesting software must not be supplied, acquired or used.

1.3 Honesty in Representation and Identity

1.3.1 User Identification

On request of relevant College managers and supervisors, a member of staff must provide evidence of their eligibility to use St Charbel’s College's IT facilities.

1.3.2 User Misrepresentation

Staff must not under any circumstance, in messages or otherwise, represent themselves as someone else, fictional or real, without providing their real identity or username.

1.3.3 Public Statements on Behalf of St Charbel’s College

Communications using College IT facilities should not give the impression that the writer is representing, giving opinions or making statements on behalf of St Charbel’s College or any part of it unless appropriately authorised to do so.
1.4 Security

The following practices should be observed to maintain the security of St Charbel’s College's IT facilities.

1. Staff must not attempt to interfere with or bypass the operation or security of IT facilities including restrictions or quotas relating to usage.
2. Staff must keep their user name and password safe and not make their password available to others or use any account set up for another user or make any attempt to find out the password of a facility or an account for which they do not have authorised access.
3. Staff must ensure that the confidentiality and privacy of data is maintained.
4. Staffs that have been granted access to computer systems are responsible for the safe keeping of data within their own area of work.
5. Staff must not divulge any confidential information that they may have access to in the normal course of their employment.
6. Staff must not seek access to data that is not required as part of their duties as a staff member of St Charbel’s College.
7. Staff who inadvertently obtains data to which they are not entitled or who become aware of a breach of security pertaining to data from any information technology facility must immediately report this to the Network Administrator. Unauthorised release or use of data inadvertently obtained may lead to legal action.
8. Staff must ensure the security of their workstation by logging off or observing other security measures when it is left unattended.
1.5 Non Interference

1.5.1 Inconvenience and Damage

Staff must not behave in a manner which, in the opinion of relevant College managers and supervisors, unduly inconveniences other people or which causes or is likely to cause damage to College IT facilities.

1.5.2 Installation of Software

Staff must not install software on any College IT facility unless the installation is designated as part of their authorised work.

2. Unacceptable or Prohibited Use of IT Facilities

2.1 Purpose

IT facilities are provided for use in St Charbel’s College's teaching and learning, research, administrative and business activities. They are not provided for private personal use, although it is recognised that, as with the telephone, there will be limited use for personal purposes (see below section 2.5).

Some types of unacceptable use, for example transmission of material of an obscene nature, are specifically prohibited by the Policy on Acceptable Use of IT Facilities and by State and Commonwealth law. Appendix A of the Policy contains relevant legislation and College policy and procedures.
2.2 Examples of Unacceptable Use

Examples of unacceptable use include:

1. Circumventing system security provisions or usage quotas.
2. Visiting inappropriate internet sites concerned with pornography and downloading materials that are pornographic or storing or transmitting any such material.
3. Playing computer games or other leisure activities such as joining in chat rooms or surfing the internet in pursuit of personal interests that are not related to work.
4. Sending or soliciting obscene, profane or offensive material (this includes accessing erotic materials via news groups).
5. Sending email messages or jokes that contain discriminating or sexually harassing material, or messages that create an intimidating or hostile work environment for others.
6. Using College IT facilities in the conduct of personal businesses or for commercial purposes that are not directly related to College business.
7. Using College email facilities to send chain letters.
8. Unauthorised forwarding of confidential College messages to persons outside St Charbel's College.
9. Using another person's mailbox without authorisation.
10. Using another's identify or concealing or misrepresenting ones name or affiliations or address.
11. Sending unsolicited personal opinions on social, political, religious or other non of College related matters, where sending such opinions is not a legitimate part of education or research.
12. Soliciting to buy or sell goods or services, except on mail groups that have been established specifically for that purpose.
13. Using, copying or transmitting copyrighted information in a way that infringes copyright.
2.3 Inadvertent Unacceptable Use

In relation to use of the web, it may not always be possible to tell if a web page is relevant until it has been read and web search engines and links can sometimes lead to irrelevant and inappropriate websites. In these cases usage logs may be used to demonstrate that access to inappropriate sites was inadvertent.

2.4 Seeking Advice on Use

Where staff has doubt concerning their authorisation to use any IT facility or about whether a particular use is acceptable, they should seek the advice of College’s Network Administrator.

2.5 Use for Personal Purposes

There may be some use of College IT facilities for personal purposes that are unrelated to work (eg internet banking). Such use must be limited, reasonable and appropriate and it must not:

1. contravene College policy or State or Commonwealth laws
2. interfere with official use of IT facilities or
3. interfere with a staff member's obligations to St Charbel’s College.

The amount of personal use is at the discretion of a staff member’s supervisor or manager and therefore, seeks advice from them about using the internet for personal purposes. For information about how use of the internet is monitored, see section 3 on Privacy and section 4 of use of IT facilities.

2.6 What to Do When Misuse is Observed

If a misuse of IT facilities is witnessed report the incident directly to the Network Administrator.
2.7 What Happens Following a Report of Alleged Misuse

Where an alleged misuse has been reported brought to the attention of the Network Administrator or staff members responsible for managing any part of St Charbel’s College’s information technology facilities, the network administrator may:

1. act immediately to prevent any continuation of the alleged misuse pending an investigation
2. promptly notify other authorities, including the relevant cost centre manager or supervisor
3. advise the person of the Acceptable Use of IT Facilities Policy and direct the person to discontinue immediately the alleged misuse.

If an investigation of alleged misuse requires a staff member's use of IT facilities to be examined or monitored they will not necessarily be notified. If the investigation of alleged misuse requires access to the contents of a staff member's computer or email, approval of the principal is required beforehand.

Allegations that constitute misconduct or breaches of the law will be referred to the appropriate authority for investigation. St Charbel’s College will give that authority all reasonable assistance requested including disclosing:

1. relevant financial and personal data, and
2. data which may be limited by contractual obligation including copyrighted software and software that is patented or which contains trade secrets
2.8 Penalties for Misuse of IT Facilities

Staff members who do not abide by College policy when using IT facilities, may have their access to IT facilities suspended or be subject to disciplinary action, or civil or criminal legal action. See the Policy on Acceptable Use of IT Facilities.

3. Privacy

3.1 Privacy Limitations

A member of staff may expect some privacy in relation to their use of the computer and email and internet resources St Charbel’s College makes available to them at work. Despite the use of individual passwords, privacy is limited in the following ways:

1. Use of computers, email and the internet can be accessed by IT administrator
2. IT systems automatically log the internet sites visited, the downloads made and the time spent at each site as well as information about emails sent and received. This automatically logged information can be accessed by the IT administrator.
3. While contents of emails and web sites are not routinely recorded, contents may be stored on staff computers or on servers.
4. It is possible to retrieve deleted records from back ups and archives.
3.2 Privacy Legislation

Besides technological limitations on privacy, there are other factors that can impinge on privacy. The Office of the Privacy Commissioner provides information on the privacy legislation and how it applies to use of IT by employees. It shows that there are exemptions to the Privacy Principles and an employer's logging of staff activities (email and internet) is not contrary to the legislation as long as it is done lawfully and fairly.

To ensure fairness, St Charbel’s College has provided these Guidelines to inform staff about its practice of monitoring and accessing records relating to use of College IT facilities, including computers, email and the internet.

For information about how St Charbel’s College protects the privacy of information it holds in relation to its students, see the Policy on Confidentiality of Student Information.

St Charbel’s College also informs members of the public about how St Charbel’s College monitors their use of St Charbel's College web site.

3.3 Freedom of Information

Another limitation on privacy arises from St Charbel’s College's obligation to comply with Freedom of Information legislation.

Under the Freedom of Information (FOI) NSW, a document is defined as anything in which information is stored or from which information may be reproduced. Email messages created in the course of fulfilling duties relating to employment are official records covered by the State Records Act (1997) and the Freedom of Information Act (1991) (FOI Act), and are subject to the same requirements as hardcopy records. The content of email messages arising from this use remains the property of St Charbel’s College and may be subject to release in accordance with the FOI Act.
4. Monitoring of Use of IT Facilities

4.1 Routine Monitoring

St Charbel’s College provides IT facilities for use by staff in relation to St Charbel’s College's teaching and learning, research, administrative and business activities. Routine monitoring of the use of IT facilities is conducted to monitor the costs and acceptable use of College resources. The type of information automatically collected includes:

<table>
<thead>
<tr>
<th>Internet</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Name of the person who accessed the internet site.</td>
<td>1. Email address of the person who sent the message.</td>
</tr>
<tr>
<td>2. Date and time the site was accessed</td>
<td>2. Name of the person who received the message.</td>
</tr>
<tr>
<td>3. Site address (or “URL”).</td>
<td>3. Email addresses of other people who received the message.</td>
</tr>
<tr>
<td>4. Computer the person used to access the internet.</td>
<td>4. Date and time at which the message was sent and received.</td>
</tr>
<tr>
<td>5. Size of the site or web page accessed or the amount of material downloaded.</td>
<td>5. Server(s) from which the message was sent.</td>
</tr>
</tbody>
</table>

St Charbel’s College routinely monitors the level of usage to control costs. Cost centres contribute towards these costs and cost centre managers receive summary information that allows them to monitor usage by staff in their cost centre. The costs associated with individual use of IT resources, specifically an individual's use of the internet.

Under the GST legislation, use of College resources for other than College business requires apportionment to determine what part of the GST paid for the goods or service can be claimed back by St Charbel’s College. This is another reason why use of College internet or email or other IT facilities for personal
purposes must only be incidental and why compliance with law may require St Charbel’s College to monitor and inspect records of use.

**4.2 Other Monitoring**

In normal circumstances, staff supporting IT services will not monitor the contents of electronic mail messages or other communications or files they access as a result of their work (eg auditing operations). However, whenever the Principal decides it is appropriate, St Charbel’s College will inspect copy, store and disclose the contents of email to prevent or correct improper use, satisfy a legal obligation, or to ensure proper operation of IT facilities.

**5. Email Bulletins and Distribution Lists**

**5.1 General Notices**

General notice bulletins to public groups, news groups, or specific work groups can only be sent for the purposes of College business associated with work. Staff must comply with the Public Statements by College Staff Policy as well as with the provisions of the Spam Act.

**5.2 All Staff Notices and All Student Notices**

To reduce the amount of unwanted and unsolicited email received by staff, approval of the intended message must be obtained from a manager who has approval to send to these lists.

**6. Other Information**

To help staff use IT resources responsibly, the following information is provided.

**6.1 Charging for Internet Use**

Generally, St Charbel’s College is charged for use of the internet involving external internet sites. It is not charged for use involving only sites within St Charbel’s College. Each area of St Charbel’s College pays for the internet use of staff. The more internet sites a staff member views and the more material downloaded, the more an organisational area pays.
As a result, heads or managers of areas have online access to information regarding the amount and cost of internet use for each individual or group of computers in their area. If a member of staff has used the internet more than expected given the staff member’s role, the Network Administrator can request to provide the details of the internet sites the individual has accessed. If the Network Administrator believes the amount of use and/or the content of some sites is inappropriate, the matter may be raised with the individual.

**6.2 How to Reduce the Cost of Internet Use**

The most common use of the internet is for accessing World Wide Web sites. Cost can be minimised by following this advice:

1. Do not leave a web browser open on a page that automatically refreshes content, particularly pictures and images.
2. Some web pages continually update themselves, usually with advertisements. Search engines, web-cams, the White Pages and Yellow Pages are typical examples. Do not leave a browser on these pages any longer than necessary.
3. Note that if a page is minimised, or hidden behind another window on the screen, the material is still being downloaded and St Charbel’s College is paying for it. It is better to close all browser windows.
4. Some web sites open additional windows behind the main one. While surfing the web, check for unwanted web browser windows, and close them.
5. Use St Charbel’s College provided email account, instead of services like Yahoo! or Hotmail, for College-related email. The inbox on St Charbel’s College email account uses St Charbel’s College’s internal network. Consequently, St Charbel’s College is not charged for that use. Reading an inbox on most other commercial email services (including Hotmail and Yahoo!) uses the internet, and St Charbel’s College will be charged for the use.
6. Consider the content of the sites visited. Web pages that contain images, movies and sound are larger, and cost more to download, than pages which are more text-oriented.
7. Configure the browser so that, by default, it does not display images.
8. Logout from the computer when finished working.
9. Use secure passwords to prevent others using the computer.

**6.3 Procedures Relating to Email When a Staff Member Leaves**

When a staff member's email account is to be deleted (because they are leaving St Charbel’s College), the person requesting the deletion must complete the appropriate form and have it authorised by the relevant Faculty Coordinator or Unit. Email accounts for people who have recently left, are shown in the address book with "Left" after their name.

1. It is the responsibility of the departing staff member to tidy up their email account prior to their departure. Messages which relate to College business should be retained or archived appropriately. Messages which remain in the email account will be viewed by other staff once the departing staff member has left.

2. Deleted email accounts actually remain active for a period of three months. During this time all email addressed to the mailbox is redirected to the member of staff who requested the deletion or their delegate. This person then has the responsibility for managing that mail.

3. New messages which arrive for a deleted email account in the three month period will not be automatically redirected to an email account external to St Charbel’s College. Personal mail messages for the former staff member will be forwarded (if a forwarding email address is known) on request of the departing staff member. College related email messages will not be disclosed nor forwarded to the former staff member.

4. After three months, the entire mailbox for the former staff member will be archived and then deleted from the address book.

5. Archived messages may be recovered for up to 12 months by submitting a formal request to the Network Administrator stating the reasons for recovery and the date/period of the mail messages to be recovered. This service may incur a fee depending on how much work is required to archive the required messages.
Guidelines for Students on Use of IT Facilities, Including Email and the Internet

These guidelines provide clarification for students on the practical application of the College's Policy on Acceptable Use of IT Facilities and they should be read in conjunction with it.

IT facilities includes all computing and communication equipment, software, services, data and dedicated building space used in connection with information technology, which is owned by, leased by or used under license or agreement by St Charbel’s College.

1. Responsibilities of students

The following sections set out requirements that are particularly significant and provide relevant information about some of the legislation that governs the use of IT facilities. All students who use College IT facilities must comply with the policy, legislation and principles that are referred to here as well as to other directives from the Director of Information Strategy and Technology Services that may be issued.

1.1 Acceptable Use of IT facilities

Information technology facilities may be used only as set out in the College's Policy on Acceptable Use of IT Facilities.

Students must not use IT facilities for the purpose of personal profit making or for commercial activities other than those of St Charbel’s College. Student use of College IT facilities including email and the internet is conditional upon compliance with all College policies procedures and guidelines, including the Sexual Harassment Policy and Grievance Procedures and Equal Opportunity Policy as well as with State and Commonwealth laws.

A list of relevant documents and Government legislation with which staff must comply is set out in Appendix A of the Policy on Acceptable Use of IT Facilities.
1.2 Copyright Law

Copyright law restricts the copying of software and other material subject to copyright (documents, music, broadcasts, videos, etc) except with the express permission of the copyright owner.

Material, including images and text, are protected by the Copyright Act of Australia. There is no general right for users of copyright material to make digital copies of copyright material. If you wish to load copyright material onto any Web Pages specific permission will need to be sought from the copyright owner. Authors of works are granted copyright protection in Australia as soon as the material expression has been created; there is no legal requirement to register the work.

If the work is created in the course of your employment then the employer will own the copyright.

St Charbel’s College accepts that in accessing these pages:

- you may retrieve material for information only
- you may save or download a local copy for personal use
- you may send it to your printer for personal use or to communicate the information to authorised and potential users, but you may not make any charge for such use
- any commercial exploitation is expressly prohibited
- you must clearly acknowledge the source by including the copyright notice in any copy you make
- you may not make any modification to the material without the express permission of St Charbel’s College, Punchbowl.
1.2.1 Software

Students may not make use of, or copy, software contrary to the provisions of any agreement entered into by St Charbel's College. The onus is on students to consult with Network Administrator to clarify the permitted terms of use if they wish to use any software for purposes other than those for which St Charbel’s College has a license.

1.2.2 Email and Copyright

The copyright of an email message is owned by the sender, or the sender's employer. Consider the expectations of the originator; did that person set any conditions on the further communication of their email, or expect that it would not be forwarded to anyone else, or would not be forwarded to a particular recipient.

1.2.3 Spam Act 2003

All email messages sent from a College email account must comply with the Spam Act 2003. This Act sets up a scheme for regulating commercial email and other types of commercial electronic messages. The Spam Act refers to spam as “unsolicited commercial electronic messaging”. “Electronic messaging” includes emails, instant messaging, SMS and other mobile phone messaging. A single message may be spam. The message does not need to be sent in bulk, or received in bulk.

1.3 Honesty in Representation and Identity

1.3.1 User Identification

On request of relevant College managers and supervisors, a student must provide evidence (eg current student ID card) of their eligibility to use St Charbel’s College's IT facilities.

1.3.2 User Misrepresentation

Students must not under any circumstance, in messages or otherwise, represent themselves as someone else, fictional or real, without providing their real identity or username.
1.3.3 Public Statements on Behalf of St Charbel’s College

Communications using College IT facilities should not give the impression that the writer is representing, giving opinions or making statements on behalf of St Charbel’s College or any part of it unless appropriately authorised to do so.

1.4 Security

The following practices should be observed to maintain the security of St Charbel’s College's IT facilities.

1. Students must not attempt to interfere with or bypass the operation or security of IT facilities including restrictions or quotas relating to usage.
2. Students must keep their username and password safe and not make their password available to others or use any account set up for another user or make any attempt to find out the password of a facility or an account for which they do not have authorised access.
3. Students must ensure that the confidentiality and privacy of data is maintained.
4. Students must not seek access to data that is not required as part of their study.
5. Students who inadvertently obtain data to which they are not entitled or who become aware of a breach of security pertaining to data from any information technology facility must immediately report this to relevant teacher or Network Administrator. Unauthorised release or use of data inadvertently obtained may lead to legal action.

1.5 Non Interference

1.5.1 Inconvenience and Damage

Students must not behave in a manner which, in the opinion of relevant College managers and staff, unduly inconveniences other people or which causes or is likely to cause damage to College IT facilities.
1.5.2 Installation of Software

Students must not install software on any College IT facility.

2. Unacceptable or Prohibited Use of IT Facilities

2.1 Purpose

IT facilities are provided for use in St Charbel’s College's teaching and learning, research, administrative and business activities. Some types of unacceptable use, for example transmission of material of an obscene nature, are specifically prohibited by the Policy on Acceptable Use of IT Facilities and by State and Commonwealth law. Appendix A of the policy contains relevant legislation and College policy and procedures.

2.2 Examples of Unacceptable Use

Unacceptable use of IT facilities is set out in section 5.3 of the Policy. Further examples of unacceptable use include:

1. circumventing system security provisions or usage quotas
2. visiting inappropriate Internet sites concerned with pornography and downloading materials that are pornographic or storing or transmitting any such material
3. sending or soliciting obscene, profane or offensive material (this includes accessing erotic materials via news groups)
4. sending email messages or jokes that contain discriminating or sexually harassing material, or messages that create an intimidating or hostile work environment for others
5. using College IT facilities in the conduct of personal businesses or for commercial purposes
6. using College email facilities to send chain letters
7. unauthorised forwarding of confidential College messages to persons outside St Charbel’s College
8. using another person's mailbox without authorisation
9. using another's identity or concealing or misrepresenting one's name or affiliations or address
10. ending unsolicited personal opinions on social, political, religious or other non College related matters, where sending such opinions is not a legitimate part of study
11. soliciting to buy or sell goods or services, except on mail groups that have been established specifically for that purpose
12. using or transmitting copyrighted information in a way that infringes the copyright.

2.3 Inadvertent Inappropriate Use

In relation to use of the web, it may not always be possible to tell if a web page is relevant until it has been read and web search engines and links can sometimes lead to irrelevant and inappropriate websites. In these cases usage logs may be used to demonstrate that access to inappropriate sites was inadvertent.

2.4 Seeking Advice on Use

Where a student is in doubt concerning their authorisation to use any IT facility or about whether a particular use is acceptable, they should seek the advice of their teacher or Network Administrator.

2.5 What to Do When Misuse is Observed

If a misuse of IT facilities is witnessed, report the incident directly the Network Administrator.

2.6 What Happens Following a Report of Alleged Misuse

Where an alleged misuse has been reported to a teacher or brought to Network Administrator or staff members responsible for managing any part of St Charbel’s College's information technology facilities, the nominee may:

1. act immediately to prevent any continuation of the alleged misuse pending an investigation
2. promptly notify other authorities, including the relevant Coordinator
3. advise the student of the Acceptable Use of IT Facilities Policy and direct the student to discontinue immediately the alleged misuse.

If an investigation of alleged misuse requires a student's use of IT facilities to be examined or monitored they will not necessarily be notified.

Allegations that constitute misconduct or breaches of the law will be referred to the appropriate authority for investigation. St Charbel’s College will give that authority all reasonable assistance requested including disclosing:

1. relevant financial and personal data, and
2. data which may be limited by contractual obligation including copyrighted software and software that is patented or which contains trade secrets.

2.7 Penalties for Misuse of IT Facilities

If a student does not abide by College Policy when using IT facilities, access to IT facilities may be suspended and disciplinary action, or civil or criminal legal action may be taken. See the Policy on Acceptable Use of IT Facilities.

3. Privacy

3.1 Privacy Limitations

The use of individual password may suggest that privacy is ensured. However, privacy is limited in the following ways.

1. Use of computers, email and the internet can be accessed by IT administrators.
2. IT systems automatically log the internet sites visited, the downloads made and the time spent at each site as well as information about emails sent and received. This automatically logged information can be accessed by the IT administrators.
3. While contents of emails and web sites are not routinely recorded, contents may be stored on staff computers or on servers.
4. It is possible to retrieve deleted records from back ups and archives.
3.2 Freedom of Information

Another limitation on privacy arises from St Charbel’s College's obligation to comply with Freedom of Information legislation.

Under the Freedom of Information (FOI) Act of NSW, a document is defined as “anything in which information is stored or from which information may be reproduced”. Email messages created in the course of studying may be official records covered by the *State Records Act 1997* and the *Freedom of Information Act 1991* (FOI ACT), and as such are subject to the same requirements as hardcopy records. The content of email messages arising from this use remains the property of St. Charbel’s College and may be subject to release in accordance with the FOI Act.

4. Monitoring Use of IT Facilities

4.1 Routine Monitoring

St Charbel's College provides IT facilities for use in relation to St Charbel’s College's teaching and learning, research, administrative and business activities. Routine monitoring of the use of IT facilities is conducted to monitor the costs and acceptable use of College resources. The type of information automatically collected includes:

<table>
<thead>
<tr>
<th>Internet</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Name of the person who accessed the internet site.</td>
<td>1. Email address of the person who sent the message.</td>
</tr>
<tr>
<td>2. Date and time the site was accessed.</td>
<td>2. Name of the person who received the message.</td>
</tr>
<tr>
<td>3. Site address (or “URL”).</td>
<td>3. Email addresses of other people who received the message.</td>
</tr>
<tr>
<td>4. Computer the person used to access the Internet.</td>
<td>4. Date and time at which the message was sent and received.</td>
</tr>
<tr>
<td>5. Size of the site or web page accessed or the amount of material downloaded.</td>
<td>5. Server(s) from which the message was sent.</td>
</tr>
</tbody>
</table>
4.2 Other Monitoring

In normal circumstances, staff supporting IT services will not monitor the contents of electronic mail messages or other communications or files they access as a result of their work (eg auditing operations). However, St Charbel’s College will inspect copy, store and disclose the contents of email when appropriate to prevent or correct improper use, satisfy a legal obligation, or to ensure proper operation of IT facilities.
Appendix A

1. Associated Documents

For information on the application of this policy see:

- Guidelines for Staff on Use of IT Facilities including Email and the Internet (page-11)
- Guidelines for Students on Use of IT Facilities including Email and the Internet (page-27)

2. Relevant Legislation

While not an exhaustive list, the following legislation is of particular relevance to the use of College IT facilities:

- Copyright Act 1968 (Cth)
- Crimes Act 1914 (Cth)
- Criminal Code Act 1995 (Cth)
- Cybercrime Act 2001 (Cth)
- Racial Vilification Act 1996 (NSW)
- Spam Act 2003 (Cth).

3. Relevant Terms

Disciplinary Procedures:

- outlined in the applicable industrial instrument shall apply to staff.
- outlined in the applicable statute or policy shall apply to students.

Industrial Instrument refers to the applicable Enterprise Agreement, Award, and Australian Workplace Agreement, contract of employment or legislation.