Communication Devices Policy

ST CHARBEL’S COLLEGE
Communication Devices Policy

Communication Devices Staff Use Policy

St Charbel’s College employees must be efficient, economical and ethical in their use and management of College resources. Communication devices, such as telephones, computers, facsimiles, the College Intranet, the Internet and email are resources provided for business and educational purposes, and all employees have a responsibility to ensure their proper and secure use. Use of the Communication devices must comply with state and federal laws. Employees must not engage in any use that may be considered questionable, controversial, offensive, or could potentially damage the College’s reputation.

Unlawful Use

Using communication devices to seek out, access, store or send any material of an offensive, obscene, pornographic, threatening, abusive or defamatory nature is prohibited and may result in disciplinary action and on occasion criminal prosecution. Employees who receive any threatening, intimidating or harassing telephone calls or electronic messages should immediately report the incident to their supervisor (for example Deputy Principal, Stage Co-ordinator, Head of Department).

Economic Use

Employees are required to use the most economical and efficient means of communication when using College communication devices. Employees should keep short any communication which is time charged; this applies equally to calls made from standard telephones as well as calls from mobile telephones. To reduce unnecessary power consumption of computer equipment, employees should completely shut down their workstation before leaving work for the weekend.

Copyright

Software, correspondence and other material copied or transmitted or otherwise used by employees, in either paper or electronic form may be subject to copyright law. If employees, without permission, use or electronically transmit material, either by email or other means, that is protected by copyright they or the College may be legally liable for infringement of the copyright. Accordingly, employees must not copy, use or transmit any material in electronic form that is protected by copyright, without prior permission from the copyright owner.
Communication Devices Policy

**Privacy**

Employees must comply with the College’s Privacy Policy and the College’s Confidentiality Policy.

**Receipt of Unacceptable Material**

Employees who receive:

- Offensive material should notify their supervisor who will assess the material and take appropriate action;

- Unsolicited material from an unknown source should delete it without replying or attempting to remove their email address from any mailing list;

- Other inappropriate material from a known source should notify the sender that the material is unacceptable to the college and that they do not wish to receive it.

- Employees should report any serious incidences of the receipt of offensive or inappropriate materials to their supervisor.

**Security**

All employees with access to College communication devices, information assets and/or ICT infrastructure are responsible for protecting these assets from loss, damage or destruction.

Employees must ensure that College information in any form cannot be accessed by unauthorised persons. Particular care should be taken when college information assets are taken or used offsite on portable and hand-held devices.

Employees should be alert to the possibility that any messages and/or data conveyed through communication devices can be intercepted, altered, corrupted, traced or recorded. While such practices are normally illegal, there can be no absolute expectation of privacy.

**Password Security**

Access to all College networks, applications and email systems is protected by password. Employees must never share their passwords with anybody, including supervisors, other staff, colleagues, students and family members.

Employees that become aware that a password may have become known to others or that their accounts have been used inappropriately, should immediately change their password and advise their supervisor.

Employees should also contact their supervisor if they are approached by someone, in person or electronically, asking them to disclose their password/account details. In most circumstances, it is impossible to determine who physically wrote an email message or accessed an application or data system. Therefore, employees will be held accountable for all activity on the College’s network, applications or data systems that has been accessed using their account User ID and password.
Communication Devices Policy

Educational Workstation Security

Educational workstations include computers that are commonly used by many people, including staff, students and parents, and are located in classrooms, libraries, staffrooms and other spaces to which students have regular access. Employees should never leave an educational workstation unattended while it is logged on to the College’s network or applications. They should close all applications and log out of any educational workstation when they have finished using it.

Employees may be required to use their personal User ID and password to log on to a shared educational workstation, such as a computer connected to a data projector or interactive whiteboard. Employees should carefully monitor the use being made of any shared educational workstation to which they have provided their User ID and password.

Employees must not use their personal User ID and password to log on to the College’s network, applications or data systems, including the College’s Internet service, for the purpose of intentionally providing students or other staff members with access to applications or systems for which they have not been authorised.

Network Security

Network data backups, operating system security updates and virus protection software updates and scans are carried out on all network computers. To make sure that these important processes operate effectively, employees must log out of or shut down their workstation at the end of each day. Employees should not tamper with or disable data backups, security updates or virus protection updates and scans.

Unacceptable Use

Any use of the College’s communication devices or services that may be considered questionable, controversial, offensive or that could potentially damage the College’s reputation or financial position is unacceptable. Any intentional unacceptable use may result in disciplinary action. These standards apply whenever College equipment or communication lines are used, even if accessed from offsite or when using a private account or device.

Unacceptable use includes but is not limited to:

- Intentionally creating, accessing, storing or transmitting information that could be reasonably considered to:
  - Be obscene, pornographic, sexually explicit or contain images of nudity;
  - Be misleading or deceptive;
  - Be threatening, abusive or defamatory;
Communication Devices Policy

- Result in victimisation, harassment discrimination or vilification;
- Lead to criminal penalty or civil liability;
- Transmitting personal correspondence to a child or young person expressing sexual feelings for that or another child or young person;
- Engaging in correspondence on social networking sites pertaining to the college, students of the college, the families of students or college colleagues;
- Discussing school matters on social networking sites (this clause is not intended to prohibit professional or educational online discussions);
- Accepting students as 'friends' on social networking sites;
- Collecting personal information not relevant to the functions of the college;
- Transmitting personal information, collected or held by the college, for any purpose other than that for which it was collected;
- Intentionally gathering, by any means, or using other users' password information for any college network access, corporate application or email account;
- Attempting to access any college online resource (data or system) without specific authority;
- Intentionally bypassing the college’s internet filtering services;
- Sharing a password for any college network access, application or email account with others;
- Intentionally giving students or other staff members access to applications or data systems, including the college’s internet service, to which they have not been authorised by logging on to the college’s network, corporate applications or data systems at multiple workstations;
- Using the college’s communication devices or services for gambling or any private income-generating purposes;
- Transmitting, without permission, any material protected by copyright;
- Copying or installing unlicensed software or downloading unauthorised software;
- Publishing or uploading materials to an internet site not associated with work;
- Downloading large graphic, audio or video files or accessing online video or audio content or occupying college data storage with data not associated with work;
- Excessively using the internet for purposes not associated with work,
Communication Devices Policy

- Accessing chat lines or instant message services not associated with work;
- Sending frivolous or unsolicited programs or email, including chain letters and unsolicited commercial email (also known as spam); or transmitting inappropriate jokes.
- Damaging or disabling computers, computer systems or networks of the college.

Personal Use

The College acknowledges that family and community responsibilities impact on work. It therefore accepts that its communication devices need to be used for personal reasons from time to time. Such use should be infrequent, brief, involve minimal cost and should not interfere with the performance of work, impact on the College’s service delivery, or create an exposure for the College to viruses, legal liability or embarrassment.

Employees making personal use of the College’s communication devices do not have the same personal privacy rights as they would have when using private or public (e.g. coin or card operated telephone) communication devices. Employees reasonably suspected of abusing their personal use of College communication devices will be asked to explain such use.

Reasonable personal use of the Internet and email is a privilege and should be consistent with such use of the telephone. Personal use of the Internet does not extend to intentionally downloading unauthorised software or large graphic, audio or video files or accessing video or audio content not associated with work. Such use must be kept to a minimum during working hours.

Employees may be held accountable for the inappropriate use of any communication device assigned to them by the College, including inappropriate use by third parties.

Monitoring Procedures

The electronic information that is sent and received via the College’s communication devices is College property. The College reserves the right to monitor all activity as a precaution against inappropriate use, such as fraud, workplace harassment or breaches of confidentiality by employees.

The College conducts surveillance and monitoring of its computer systems to ensure the ongoing confidentiality, integrity and availability of business and education systems. Employees provided with mobile communication devices by the College are advised that the use of those devices may be monitored to ensure that calls designated as work and private are correctly recorded and accounted for.
Communication Devices Policy

**Communication Devices Student Use Policy**

The internet provides an opportunity to enhance students’ learning experiences by providing access to vast amounts of information across the globe. Online communication links students to provide a collaborative learning environment and is intended to assist with learning outcomes. Today’s students are exposed to online communication tools and the internet in their community.

Use of computers, the internet and online communication services provided by St Charbel’s College is intended for research and learning and communication between students and staff. Access to internet and online communication tools at school will assist students to develop the information and communication skills necessary to use the internet effectively and appropriately.

Responsible use of the services by students, with guidance from teaching staff, will provide a secure and safe learning environment.

Students using internet and online communication services have the responsibility to report inappropriate behaviour and material to their teacher.

Students who use the internet and online communication services provided by St Charbel’s College must abide by the College’s conditions of acceptable usage, see Communications Devices User Consent Form provided in the College’s enrolment package. Students should be aware that a breach of this policy may result in disciplinary action in line with the school’s discipline policy.

Students will:

- Not disable settings for virus protection, spam and filtering that have been applied as the College’s standard.
- Ensure that communication through internet and online communication services is related to learning.
- Keep passwords confidential, and change them when prompted, or when known by another user.
- Use passwords that are not obvious or easily guessed.
- Never allow others to use their personal e-learning account.
- Log off at the end of each session to ensure that nobody else can use their e-learning account.
- Promptly tell their supervising teacher if they suspect they have received a computer virus or spam (i.e. Unsolicited email) or if they receive a message that is inappropriate or makes them feel uncomfortable.
Communication Devices Policy

- Seek advice if another user seeks excessive personal information, asks to be telephoned, offers gifts by email or wants to meet a student.

- Never knowingly initiate or forward emails or other messages containing:
  
  - A message that was sent to them in confidence.
  
  - A computer virus or attachment that is capable of damaging recipients' computers.
  
  - Chain letters and hoax emails.
  
  - Spam, e.g. Unsolicited advertising material.

- Never send or publish:
  
  - Unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
  
  - Threatening, bullying or harassing another person or making excessive or unreasonable demands upon another person.
  
  - Sexually explicit or sexually suggestive material or correspondence.
  
  - False or defamatory information about a person or organisation.

- Ensure that personal use is kept to a minimum and internet and online communication services is generally used for genuine curriculum and educational activities.

- Not use unauthorised programs or intentionally download or upload unauthorised software, graphics or music that is not associated with learning.

- Never damage or disable computers, computer systems or networks of the College.

- Ensure that services are not used for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.

- Be aware that all use of internet and online communication services can be audited and traced to the e-learning accounts of specific users.

Privacy and Confidentially

Students will:

- Never publish or disclose the email address of a staff member or student without that person's explicit permission.
Communication Devices Policy

- Not reveal personal information including names, addresses, photographs, credit card details and telephone numbers of themselves or others.

- Ensure privacy and confidentiality is maintained by not disclosing or using any information in a way that is contrary to any individual's interests.

Intellectual Property and Copyright

Students will:

- Never plagiarise information and will observe appropriate copyright clearance, including acknowledging the author or source of any information used.

- Ensure that permission is gained before electronically publishing users’ works or drawings. Always acknowledge the creator or author of any material published.

- Ensure any material published on the internet or intranet has the approval of the principal or their delegate and has appropriate copyright clearance.

- Not use illegally acquired software.

Misuse and Breaches of Acceptable Usage

Students will be aware that:

- They are held responsible for their actions while using internet and online communication services.

- They are held responsible for any breaches caused by them allowing any other person to use their e-learning account to access internet and online communication services.

- The misuse of internet and online communication services may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services.

Monitoring, evaluation and reporting requirements

Students will report:

- Any internet site accessed that is considered inappropriate.

- Any suspected technical security breach involving other users both from within or outside the college.
Communication Devices Policy

**Copyright: podcasting in schools**

This policy applies to all staff and students at St Charbel's College.

Before downloading or viewing a podcast staff in schools should check the podcasters terms and conditions and ensure they are permitted to use the podcast for ‘educational purposes’.

When a school is creating their own podcast they are required to:
- Obtain permission for the use of any material included in the podcast such as music tracks or films owned by another person.
- Obtain written consent of students (or parent/guardians) and other persons appearing in a podcast.
- When creating a podcast and using externally owned copyright material schools will generally be required to “credit” (acknowledge) the copyright owner in the final product as part of the licence agreement.