Republic of the Philippines
Department of Education
Region V(Bicol)
SCHOOLS DIVISION OFFICE OF CATANDUANES
Virac, Catanduanes

catanduanes@deped.gov.ph / catanduanesdiv15@gmail.com
www.depedrovcatanduanes.com (052)811-4063

DIVISION MEMORANDUM
No. 117 s. 2017

TO : Chief Education Supervisors –CID/SGOD
Education Program Supervisors
SDO Section Heads & Staff
Public Schools District Supervisors
Elementary/Secondary School Heads
Elementary/Secondary Teachers
All others concerned

FROM : SOCORRO V. DELA ROSA, CESO VI
Schools Division Superintendent

SUBJECT : POLICIES ON THE PROPER USE OF COMPUTERS/LAPTOP AND INTERNET/NETWORK FACILITIES IN THE SCHOOLS DIVISION OFFICE AND SCHOOLS

DATE : July 11, 2017

1. The Department of Education (DepEd) has been involved in various programs and projects aimed at modernizing its operations and improving the teaching and learning process in the schools. Among these are the **DepEd Computerization Program(DCP),** which facilitates the deployment of computer laboratories to public elementary and secondary schools, the **DepEd Internet Connectivity Program (DICP),** which provides schools internet connectivity, and **development systems,** which are used by administrative offices and public schools.

2. With these developments, increase in computer and network/internet activities leading to different concerns is expected. The Schools Division Office of Catanduanes recognizes that Information & Communication Technology (ICT) has many benefits and can make workplace communication more efficient and effective. Therefore, employees and teachers are encouraged to use ICT properly. This policy covers the appropriate use of all information resources including computer/laptop, networks, website, email addresses, and the information contained therein.

3. The objective/purpose of this policy is to prohibit certain unacceptable uses of ICT, and to facilitate the individual responsibilities in the usage of ICT system in the division.

4. To ensure effective and efficient use of computers/laptop, internet/networks facilities in the Schools Division Office and Schools, this Office is hereby issuing the following policies strictly adhere to the provisions of **DepEd Order No. 105, s. 2009** and **DepEd Order No. 95, s. 2010:**

A. *Personal Files or Software, and Equipment and Peripherals*

A.1 Personal Files or software such as documents, pictures, audio, video, etc. must not be placed, copied and installed in the DepEd-owned computers. These files must be stored in external storage devices such as optical disks, external had disks, USB flash drives owned personally by the user.

A.2 Officials, employees, students with DepEd ICT equipment and peripherals such as computers or laptop, mouse, keyboard, storage devices labeled with official DepEd property stickers can avail of technical assistance and/or repair services provided by this Department.

A.3 Personal ICT equipment and peripherals such as computers, mouse, keyboard, storage devices, among others may be used in the performance or enhancement of their duties at their own risk. They shall also be properly recorded with the School Division Security Officer/School Property Custodian.

A.4 However, in the event that these personal ICT equipment and peripherals break down, the owner **cannot avail of any technical assistance and/or repair services from DepEd hired ICT maintenance crew,** since these are not DepEd properties.

B. Security and Virus Infection Prevention

B.1 DepEd employees and students shall assume full responsibility that goes with using their computer, network and e-mail accounts.

B.2 Users should not disclose their passwords to unauthorized personnel to avid tampering with these facilities.

B.3 Copying, publishing, storing and transmitting of official data without authorization from the Office of the Planning Service shall be prohibited.

B.4 Computer users shall be instructed to update their anti-virus software daily to prevent data loss and spread of infection to the network and other computers.

B.5 Computers and other storage devices which were used for fieldwork **should be scanned first** before using to avoid possible computer virus infection, since majority of anti-virus software rely on an active internet connection. Technical assistance shall be provided by their respective ICT units, ICT coordinators or computers maintenance crew.

C. Software Installation and Issues

C.1 Only licensed and/or authorized open-source software shall be installed in DepEd-owned computers.

C.2 Installation of pirated software in DepEd-owned computers shall be strictly prohibited.

C.3 Installation and/or downloading of unauthorized software shall be strictly forbidden.

C.4 An office which has application software requirements shall coordinate with the ICT unit/ICT coordinators to make the necessary arrangements in procuring the license/s of the required software.

C.5 For software which need to be updated periodically (e.g. anti virus software), an office shall seek the assistance of its respective ICT units, ICT coordinators or computer maintenance crew.

C.6 **Watching TV programs**, through "TV Tuners", DVD videos, and **playing of games** which are not for official use, shall be **strictly prohibited.**

D. ICT Equipment Set-up

D.1 An office with new ICT equipment, which requires installation and/or connectivity of its different components, shall make arrangements with the ICT units, ICT coordinators or computer maintenance crew for proper scheduling.

E. Warranty Issues

E.1 Only office with ICT equipment and peripherals considered 'out-of-warranty' and enrolled in the current ICT equipment and peripherals shall be diagnosed and repaired by its respective ICT units, ICT coordinators or computer maintenance crew.

E.2 An office, with computers, printers and scanners that are still **within the manufacturer's/suppliers warranty period**, can **request only for diagnosis but not for repair** of these facilities by its ICT units, ICT coordinators or computer maintenance crew to avoid the cancellation of their warranty.

F. Internet

F.1 Administrative Use (Schools Division Office/Schools)

F.1.1 Internet access is only granted to a limited number of users specified by the head of office and therefore identified as authorized users.

F.1.2 Internet access is provided to employees for the purpose of study, research, service and other activities, which must be in the conduct of official business or in furtherance of the mission and purpose of DepEd.

F.1.3 Each employee using the DepEd Internet access shall identify himself/herself honestly, accurately, and completely when corresponding or participating in interactive activities.

F.1.4 Employees have no right of ownership or expectation of personal privacy as to their Internet usage.

F.1.5 The Division IT Officer are hereby designated to monitor all Internet usage including network traffic and with or without notice, to limit or restrict any employee's Internet usage privileges.

F.1.6 Offensive and/or subversive content may not be accessed, displayed, archived, stored, distributed, edited, or recorded using DepEd network, printing or computing resources.

- Offensive content includes, but not limited to -
  - ✓ Pornography, sexual comments or images, profanity, racial slurs, gender specific comment, or any content that can reasonably offend someone on the basis of sex, race, color, religion, national origin, age, sexual orientation, gender identity, mental or physical disability.
- Subversive content includes, but not limited to -
  - ✓ Lending aid, comfort and moral support to individuals, groups or organizations that advocate the overthrow of incumbent governments by force and violence on the basis of treason, sedition, sabotage, espionage or acts of terrorism.

F.1.7 Accessing of prohibited sites will be considered a violation of the DepEd Internet usage policies.

F.1.8 As part of Internet security, attempts to access these and other non-work related sites shall be discouraged and/or blocked.

F.1.9 The Division IT Officer are instructed to configure their proxy servers and/or switch routers in order to filter/block prohibited sites (if applicable).

F.1.10 All sites that are visited and revisited by the users should be recorded for monitoring purposes.

F.1.11 Internet access shall not be used to conduct personal business, play computer games, gamble, run a business, conduct political campaigns, activities for personal gain, or to take part in any prohibited or illegal activity.

F.1.12 No employee may use the Internet access to post messages to an Internet message board, chat room, 'web blog', 'listserv', or other Internet communication facility, except in the conduct of official business or furtherance of the DepEd mission.

F.1.13 No employee may use DepEd facilities knowingly to download or distribute pirated software and/or data. Any software or files downloaded via the Internet may be used only in ways that are consistent with their licenses or copyrights.

F.1.14 No employee may use the DepEd Internet facilities to deliberately propagate any virus, worm, Trojan horse, trap-door, or back-door program codes or knowingly disable or overload any computer system, network, or to circumvent any system intended to protect the privacy or security of another user.

F.2 Classroom Instruction Use (Schools)

F.2.1 Internet access is provided to teachers and students for the purpose of study, research, and other services/activities, which must be in the conduct of classroom instruction.

F.2.2 Internet access is only granted to a limited number of teachers or students specified by the School Head/School ICT Coordinator and therefore identified as authorized users.

F.2.3 Each teacher and student using the school's Internet access shall identify themselves honestly, accurately, and completely when corresponding or participating in interactive activities.

F.2.4 Teachers and students have no right to ownership or expectation of personal privacy as to their Internet usage.

F.2.5 The School Information Communication Technology (ICT) Coordinator is hereby designated to monitor all Internet usage including network traffic and with or without notice, to limit or restrict any teacher's/student's Internet usage privileges.

F.2.6 Offensive and/or subversive content may not be accessed, displayed, archived, stored, distributed, edited, or recorded using the schools' network, printing or computing resources.

- Offensive content includes, but not limited to -
  - ✓ Pornography, sexual comments or images, profanity, racial slurs, gender specific comment, or any content that can reasonably offend someone on the basis of sex, race, color, religion, national origin, age, sexual orientation, gender identity, mental or physical disability.
- Subversive content includes, but not limited to -
  - ✓ Lending aid, comfort, and moral support to individuals, groups or organizations that advocate the overthrow of incumbent governments by force and violence on the basis of treason, sedition, sabotage, espionage or acts of terrorism.

F.2.7 Accessing of prohibited sites will be considered a violation of the DepEd Internet usage policies.

F.2.8 As part of Internet security, attempts to access these and other non-educational related sites shall be discouraged and/or blocked.

F.2.9 School ICT Coordinators are instructed to configure their proxy servers and/or switch routers in order to filter/block prohibited sites (if applicable).

F.2.10 All sites that are visited and revisited by the teacher/student should be recorded for monitoring purposes.

F.2.11 Internet access shall not be used to conduct personal business, play computer games, gamble, run a business, conduct political campaigns, activities for personal gain, or to take part in any prohibited or illegal activity.

F.2.12 No teacher or student may use the Internet access to post messages to an Internet message board, chat room, 'web blog', 'listserv', or other Internet communication facility, except in the conduct of educational purposes or furtherance of the school's mission.

F.2.13 No teacher or student may use the school's facilities knowingly to download or distribute pirated software and/or data. Any software or files downloaded via the Internet may be used only in ways that are consistent with their licenses or copyrights.

F.2.14 No teacher and/or student may use the school's Internet facilities to deliberately propagate any virus, worm, Trojan horse, trap-door, or back-door program codes or knowingly disable or over load any computer system, network, or to circumvent any system intended to protect the privacy or security of another user.

F.2.15 Before the students can access the Internet, an orientation meeting between the students, parent/s or guardian and teachers must be organized and carried out. In this event, discussions will focus on what are the roles for each of the parties involved and have an understanding on what are the benefits and risks that exist online, as well as how to surf safely and responsibly.

G. SCHOOLS DIVISION OFFICE EMAIL ADDRESSES / WEBSITE

It is now required that every government agency must have their own website to support an effective, transparent and accountable governance and, in particular, support the speedy enforcement of rules and delivery of accessible public services to the people. And to take full advantage of the system, the Schools Division Office hereby formulates the following rules and obligations of concerned personnel:

- Section Chiefs/Heads, Education Program Supervisors, Cluster Supervisors and School Heads are advised to provide a hard and soft copy of narrative report with pictures on their latest programs, trainings, projects, winnings, accomplishments, undertakings, events/happenings, copy of SIP, and enrolment.

- Section Chiefs/Heads, Planning Officer and Alternative Learning System Staff are likewise advised to provide a hard and soft copy of the latest Division Profile, eBEIS, accomplishments, performance indicators, SIP, enrolment, directories, seminars and trainings, employee profiles, and other documents.

- Record Section and SDS office staffs/secretaries must furnish the Website Personnel/ IT Officer a soft copy of every latest division memorandum, advisories, bulletins, letters and the like, always in advance to facilitate dissemination to all clientele.

- The Division IT Officer must upload only necessary information about the Division and Schools without violating rules and regulations on Website Law.

- Publishing of news and articles must be reviewed by the assigned editor(s) or by the Filipino and English Supervisors and approved by the SDS.
- The following are the official email addresses/website of the Schools Division Office of Catanduanes:
  - catanduanes@deped.gov.ph/catanduanesdiv15@gmail.com
  - www.depedrovcatanduanes.com

For information, guidance and compliance.