# CONTRACT AND DATA PRIVACY CONSENT

Dear Parent/Guardian,

As technology is a more widely used form of communication with parents and the wider community, we must be aware also of the privacy factors of everyone and especially keep the best interest of the students in mind.

- Please read this page carefully as it includes information about safety and security issues associated with privacy.

The school respects your child's right to privacy and aims to comply with the requirements of all relevant privacy and data protection laws, particularly the Data Privacy Act of 2012. In the interest of safety and security, the School requires parent permission for the publishing of your child's Personal Information such as names, photographs and videos on all school publications whether it is our own websites, Facebook page, newsletters, or material published about the School by outside organizations.

We believe it is important to celebrate children's achievement, but are aware of the potential risks when such Personal Information or material is published on a global information system such as the Internet. Moreover, at RCAMES Cluster 5&6, we use G Suite for Education, and we are seeking your permission to provide and manage a G Suite for Education account for your child.

G Suite for Education is a set of education productivity tools from Google including Gmail, Calendar, Docs, Classroom, and more used by tens of millions of students and teachers around the world. At our institution, students will use their G Suite accounts to complete assignments, communicate with their teachers, and learn 21st century digital citizenship skills.

Please indicate your wishes by ticking the relevant box below:

| YES | NO | ***I give permission for my child's name, photograph and/or video to appear in school publications such as:*** |
|---|---|---|
| □ | □ | Newsletter; |
| □ | □ | School Official Website; |
| □ | □ | School Official Social media page; |
| □ | □ | School Newspaper article/gazette/publication; |
| □ | □ | Broadcasting program about the school (via Radio or Television). |

□ □ I give permission to create/maintain a G Suite for Education account for my child and for Google to collect, use, and disclose information about my child only for the purposes described in the notice stated in the Data Privacy Policies.

Note: Please ensure that you have discussed this with your child and that he/she understands the importance of Privacy and cyber safety issues surrounding the use of online material.

*All information shall be used by the School for legitimate purposes specifically for above mentioned permission and shall be processed by authorized personnel in accordance with the Data Privacy Policies of the School. I hereby allow and authorize the School to use, collect and process the information for legitimate purposes specifically, and allow / authorized personnel to process the information. We have carefully read and understood all the policies, rules and regulations stipulated in this Handbook and hereby agree to abide to all provisions provided therein.*

Name of Child: ________________________________________

Grade Level and Section: ____________________________________

Parent's/Guardian's Name: _______________________________

Signature of Parent/Guardian: _______________________________

## RCAMES Privacy Policies

### I. General Data Privacy Rights

Under RA 10173, people whose personal information is collected, stored, and processed are called data subjects. Organizations who deal with your personal details, whereabouts, and preferences are duty bound to observe and respect your data privacy rights. If you feel that your personal data has been misused, maliciously disclosed, or improperly disposed, or if any of the rights discussed here have been violated, the data subject has a right to file a complaint with us.

#### A. The right to be informed

Under R.A. 10173, your personal data is treated almost literally in the same way as your own personal property. Thus, it should never be collected, processed and stored by any organization without your explicit consent, unless otherwise provided by law. Information controllers usually solicit your consent through a consent form. Aside from protecting you against unfair means of personal data collection, this right also requires personal information controllers (PICs) to notify you if your data has been compromised, in a timely manner.

As a data subject, you have the right to be informed that your personal data will be, are being, or were collected and processed. The Right to be informed is a most basic right as it empowers you as a data subject to consider other actions to protect your data privacy and assert your other privacy rights.

#### B. The right to access

This is your right to find out whether an organization holds any personal data about you and if so, gain "reasonable access" to them. Through this right, you may also ask them to provide you with a written description of the kind of information they have about you as well as their purpose/s for holding them.

Under the Data Privacy Act of 2012, you have a right to obtain from an organization a copy of any information relating to you that they have on their computer database and/or manual filing system. It should be provided in an easy-to-access format, accompanied with a full explanation executed in plain language. You may demand to access the following:

1. The contents of your personal data that were processed.
2. The sources from which they were obtained.
3. Names and addresses of the recipients of your data.
4. Manner by which they were processed.
5. Reasons for disclosure to recipients, if there were any.
6. Information on automated systems where your data is or may be available, and how it may affect you.
7. Date when your data was last accessed and modified
8. The identity and address of the personal information controller.

### C. The right to object

You can exercise your right to object if the personal data processing involved is based on consent or on legitimate interest. When you object or withhold your consent, the personal information controllers (PICs) should no longer process the personal data, unless the processing is pursuant to a subpoena, for obvious purposes (contract, employer employee relationship, etc.) or a result of a legal obligation. In case there is any change or amendment to the information previously given to you, you should be notified and given an opportunity to withhold consent.

### D. The right to erasure or blocking

Under the law, you have the right to suspend, withdraw or order the blocking, removal or destruction of your personal data. You can exercise this right upon discovery and substantial proof of the following:

1. Your personal data is incomplete, outdated, false, or unlawfully obtained.
2. It is being used for purposes you did not authorize.
3. The data is no longer necessary for the purposes for which they were collected.
4. You decided to withdraw consent, or you object to its processing and there is no overriding legal ground for its processing.
5. The data concerns information prejudicial to the data subject — unless justified by freedom of speech, of expression, or of the press; or otherwise authorized (by court of law)
6. The processing is unlawful.
7. The personal information controller, or the personal information processor, violated your rights as a data subject.

### E. The right to damages

You may claim compensation if you suffered damages due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data, considering any violation of your rights and freedoms as a data subject. The right to file a complaint with the National Privacy Commission (NPC), if you feel that your personal information has been misused, maliciously disclosed, or improperly disposed, or that any of your data privacy rights have been violated, you have a right to file a complaint with the NPC.

For more details, please type the link in your internet browser:

https://www.privacy.gov.ph/know-your-rights/
or https://www.privacy.gov.ph/30-ways/

## II. School Privacy Policies

To ensure that the rights of the data subjects are protected, the above-mentioned departments are subject to the following policies:

### A. Notification of Data Subjects

Collection of information is done with the consent of Data Subjects (students and their parents or guardians) which consent is included in the forms filled-out during application for admission, enrolment or availment of student services such as scholarships, financial assistance, etc.

Forms for collection of Personal Data include a provision or a variation of these privacy statements:

“*All information shall be used by the School for legitimate purposes specifically for ______________________ and shall be processed by authorized personnel in accordance with the Data Privacy Policies of the School.*”

“*I hereby allow/authorize the School to use, collect and process the information for legitimate purposes specifically for ______________________, and allow authorized personnel to process the information.*”

In case, there is no form or written document containing the privacy statement, the authorized personnel tasked to collect the information may verbally notify them of the purpose and ask the Data Subject to allow the School personnel to collect and process the information and shall record the Processing of information with consent in writing

### B. Access only to Authorized Personnel

Only authorized personnel are allowed to access and process the Personal Data collected from the students, their parents or guardians in accordance with Data Privacy Policies of the School which requires that student records as well as the information contained therein are to be kept confidential.

Example: Only the Registrar or the duly authorized representative or personnel is allowed complete access to the student profile which includes the name, student number, parents’ names, addresses, contact numbers, grades, academic status and the like.

### C. Necessity of Information

Authorized school personnel shall collect Personal Data which is reasonably necessary or directly related to the School’s primary or secondary functions or activities. Personal Data shall not be collected in anticipation that it may be useful in the future (“just in case” it is needed). The physical records or those which are not digital stored and secured in the School database are stored in the particular offices of each Department.

For student records from previous years which are required to be perpetually stored and maintained by the School, a warehouse in a secured location is maintained by the Physical Plant Officer (PPO) of the School tasked to physically store and secure the records. Access is restricted where such records may only be retrieved upon specific instructions of the Registrar and only for legitimate purposes or upon request of the student or alumni for copies of their individual school record or pursuant to the Registrar's procedures and policies on request for records.

Personal Data shall be collected by lawful and fair means, which is allowed under the School's policies.

### D. Accuracy of Information

a. **Verification of Information.** Authorized personnel must take reasonable steps to ensure that the Personal Data collected or processed are up-to-date, complete, relevant and not misleading. The information collected from students and personnel is verified by the particular departments collecting the information. Student information is verified by the Registrar's Office while the HRD conducts the verification of personnel information and background checks.

b. **Correction or Update of Information**. Students may update their Personal Data through forms available from the Registrar's Office. In case of erroneous or false information, the students may have the information corrected, rectified, blocked or erased (blocking and erasure only to the extent allowed by DepEd Policies on Correction of School Records and other applicable laws) using the same process.

c. **Google Suite for Education Privacy Policy.** This notice describes the personal information we provide to Google for these accounts and how Google collects, uses, and discloses personal information from students in connection with these accounts. Google provides information about the information it collects, as well as how it uses and discloses the information it collects from G Suite for Education accounts in its G Suite for Education Privacy Notice. You can read that notice online at https://gsuite.google.com/terms/education_privacy.html

## Acceptable Use Policy (AUP)

### I. Overview and Policy Statements

The use of mobile devices greatly influenced people's behavior and social interaction. Advanced mobile technology enabled man to communicate to anyone, anytime, anywhere. With this increased electronic interaction is the production of cheap, open source operating systems that make way for the creation of different applications and devices that can be used for people's daily activities.

The Pontifical Council for Social Communications in their document, The Church and the Internet (2002) confirms this role of the Internet and the emerging technologies. "Teaching about the Internet and the new technology thus involves much more than teaching techniques; young people need to learn how to function well in the world of cyberspace, make discerning judgments according to sound moral criteria about what they find there, and use the new technology for their integral development and the benefit of others."

Thus, teachers and parents should teach and guide the young to use technology the right way productively. Hence, when properly utilized, mobile technology provides a gateway for learning to occur as both the teacher and the learner discover and fulfil their roles: that of educational collaborators working for each other's development in a continuously changing information technology landscape of the world.

The policy adheres in empowering our students and teachers to use current generation electronic devices to maximize their productivity and learning; and contribute to the realization of Mission-Vision Statement and for the access to Internet and contribute broadly to educational, research, and prepares the students to meet the demands of the global society.

This embodies the fair use policy of the School IT System users. Any users connected in the network/system must conform to this policy and the stated purposes of the Acceptable Use Policies. Each network/system member is responsible for the activity of its users and for ensuring that its users are familiar with the accepted use policy or an equivalent policy. In addition, it is expected that each member will maintain and enforce its own Acceptable Use Policy. At a minimum, users of the school IT system expects such policy will include:

1. To respect the privacy of other users each will be given in the school admin console.
2. To respect the legal protection provided by copyright and license to programs and data.
3. To respect the integrity of the network/system.

II. TERMS OF THE  POLICY

1. School IT System: This is a connection of networks of the offices and departments and affiliated departments under the Office of the School Director - Educational Technology Management Office (ETMO).
2. Network Administrator: The ETMO Head together with the IT Support personnel has the system privileges and is sole responsible for the operation and security of one or more networked computing- resources and all accounts on its computer systems.
3. System User: A system user is a person who is given exclusive access by the network member to an account on school admin console. A user should only use his/her account for the purposes which it has been issued.
4. School Admin Console: a database that keeps track of all user accounts and passwords thru Google Domain Settings, Student Management System for RFID and Internet Network Access.
5. Educational Devices. These are electronic devices which can be used to enhance student learning in the classroom and perform specific tasks in regards with the educational instructions; such as Chromebook, laptop, tablets/ipads, netbooks and such which will be used.

## III. POLICIES AND GUIDELINES

The procedures and policies adapted the DepEd Order (D.O.) 105, S. 2009 – GUIDELINES IN MANAGING THE PROPER USE OF INTERNET SERVICES IN ALL ADMINISTRATIVE OFFICES AND SCHOOLS. This set of policies and guidelines has been modified and aligned to the school's capability to enforce the network system in pursuant of this order.

The Internet is a global system of interconnected computer networks that consists of millions of private and public, academic, business and government networks of local to global scope that are linked by copper wires, fiber-optic cables, wireless connections, and other technologies. A computer that connects to the Internet can access information from a vast number of servers and other documents and send information onto the network which can be saved and ultimately accessed by other servers and computers.

The Internet serves as the backbone for different applications which will be used in the School internet system but not limited to the World Wide Web (www or just the Web), Electronic Mail (email) Remote Access, File Sharing, Streaming Media, Internet Telephony (VoIP)

As the Internet is known to be a place where a lot of information can be extracted and shared to educate people, it is also filled with dangerous software/ programs (malicious software) that may steal important information, destroy or even use anybody's computer without his/her knowledge and harm others.

In order to avoid being victimized by such hazards, the School IT System, is hereby issuing the following guidelines for Classroom Instruction Use:

1. Internet access and school domain address is only granted to offices, teachers, and students specified by the EdTech Management Officer.
2. Teachers and students have no right to ownership or expectation of personal privacy as to their Account and Internet usage.
3. Internet access and school domain address 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.
4. Each teacher and student using the school's Internet access and school domain address shall identify themselves honestly, accurately, and completely when corresponding or participating in interactive activities.
5. The EdTech/IT Head Support is hereby designated to monitor all Internet and system account usage including network traffic and with or without notice, to limit or restrict any teacher's/student's Internet usage privileges. Offensive and/or subversive content may not be accessed, displayed, archived, stored, distributed, edited, or recorded using the schools' network, printing or computing resources:
    a. Phishing. Do not exploit Google Classroom or use it for purposes other than organizing, communicating or collaborating for educational or Classroom purposes. Keep our product spam and malware free, and do not use our products for phishing. Spam includes, but is not limited to, unwanted promotional or commercial content and unwanted or mass solicitation. We also do not allow the transmission of malware, viruses, destructive code, or anything that may harm or interfere with the operation of the networks, servers, or other infrastructure of Google or others. Don't use Classroom to trick, mislead, or deceive other users into sharing information under false pretenses. Refrain from soliciting or collecting sensitive data, including but not limited to passwords, financial details, and social security numbers.
    b. Trolling. Posting or commenting online in a way that is deliberately cruel, offensive, or provocative.
    c. Virtual Session Raids - Users join a discord server to cause a ruckus. Ruckus factor may also be small to large. Most common form is a people joining a server and spamming/mass pinging.

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

7. IT Support are instructed to configure their proxy servers and/or switch routers in order to filter/block prohibited sites (if applicable).

8. All sites that are visited and revisited by the teacher/student should be recorded by the Network Administrator for monitoring purposes.

9. Internet access and school domain address 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.

10. No teacher or student may use the Internet access and school domain address to post messages to an online discussion, chat room, 'web blog', 'listserv', or other Internet communication facility, except in the conduct of educational purposes or furtherance of the school's mission. All websites or applications that do not confer to this definition are not allowed in our internet connections. These websites or applications are, but not limited to

   a. All social networking websites and can be accessed using smart devices (Facebook, Instagram, Twitter, etc.)
   b. All gaming websites and mobile gaming applications
   c. All adult websites
   d. All gambling websites

11. No teacher or student may use the school's IT system facilities knowingly to download or distribute pirated software and/or data via direct download or peer-to-peer (P2P) file sharing programs, websites and/or applications. Any software or files downloaded via the Internet may be used only in ways that are consistent with their licenses or copyrights.

12. No teacher and/or student may use the school's IT system 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.

13. 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.

14. Furthermore, the school urges the personnel, parents and students to take time to read articles at www.bit.ly/unicefchildsafety which is an educational resource site whose goal is to teach individuals about Child Safety Online Global challenges and strategies.

IV. Guidelines and Policies on Online Classes

## MISBEHAVIOR AND CORRESPONDING INTERVENTIONS IN ONLINE CLASSES

### MINOR OFFENSE

INTERVENTIONS

NOTE: ALL MINOR OFFENSES WILL BE HANDLED BY THE ADVISERS/SUBJECT TEACHERS

- 1st Offense: Warning by the concerned teacher and to be documented in the Anecdotal Record
- 2nd Offense: Issuance of Case Letter by the subject teacher noted by the class adviser
- 3rd Offense: Online Parent Conference with Adviser / Teacher and Guidance Associate Counselor (Online)
    - o Continuous online counseling sessions, close monitoring of the concerned students
    - o Online Spiritual sessions with the CLEd Coordinator / CCFO Head

1. Using other's username in logging in online class.
2. Eating while online classes is ongoing.
3. Opening other websites while online class is in progress.
4. Unmuting without permission when the teacher has placed you on mute.
5. Wearing inappropriate clothes that are not suited as school wear (shorts, sleeveless, sando, miniskirts, provocative dresses etc.) while attending online classes.
6. Playing games and attending to other things while attending the period when broadcasting the distance learning period is ongoing.
7. Leaving the session without prior permission from the teacher.
8. Improper decorum during student activity (boisterous laughs, make faces, private conversations pinching nose etc.)
9. Refusing to follow the rules of the specific virtual learning classroom

### MAJOR OFFENSE

INTERVENTIONS: Students found guilty of committing any of the offenses below after due process shall be subjected to:

- 1st Offense: One-day suspension from attending online classes with one hour online counseling with the Guidance Counselor.
- 2nd Offense: Two days suspension from attending online classes with one hour counseling with the Guidance Counselor and one hour online Spiritual counseling with CLEd Coordinator

· 3rd Offense: Three days suspension from attending online classes with one hour counseling with the Guidance Counselor one hour online Spiritual counseling with CCFO Head

1. Sharing of login credentials to others.
2. Sharing the link to other students who are not participants of online class.
3. Reporting to school physically that violates quarantine protocol and without permission from school authorities
4. Posting of screen shots of the online class on social media without prior permission from the teacher
5. Sending or posting discriminating, harassing, threatening images or messages.
6. Stealing using disclosing someone else's code or password
7. Engaging in unauthorized transactions that may incur a cost to the school
8. Recording the teacher or classmates without permission.
9. Encouraging, threatening or intimidating students not to attend online periods.

10. Creating fights between and among students whether visual or written using any social media platforms,

11. Participating in audio and video conversations with other students while live broadcasting is done.

12. Making unnecessary, derogatory and offensive and disrespectful to any other user.

13. Displaying and possessing cigarettes or any smoking paraphernalia while attending online classes.

14. Deliberately changing files and other information to other students or anyone without consent of the owner .

15. Downloading software or any applications that may seem hazardous or uncalled for to the smooth discussion of the lessons. (i.e with sexual content )

16. Sharing photos, videos and data about any of the students, faculty and parents without their approval.

17. Video recording any form of conversations between students and intentionally sharing it on any social media platforms without the approval of the concerned individuals.

18. Bullying R.A 10627

Bullying shall be defined as any severe or repeated by one or more students of a written verbal or electronic expression or a physical act or gesture or any combination thereof , directed at another student that has the effect of actually causing or placing the latter in reasonable fear of physical or emotional harm or damage to his property creating a hostile environment at the school for the other student , infringing on the rights of another student at school ; or materially or substantially disrupting the education process or an orderly operation of the school such as but not limited to the following:

i. Any act that causes damage to a victim's psyche and or emotional well being

ii. Any slanderous statement or accusation that causes the victim undue emotional distress like directing foul language or profanity at the target, name calling for tormenting and commenting negatively on victim's looks, clothes or body

iii. Cruel instant computer messaging harassing, threatening or insulting emails from any social media platform or application

19. ANY FORM OF CHEATING
20. DISHONESTY/PLAGIARISM
21. ANY ACTS SIMILAR ON FOREGOING

**GRAVE OFFENSE**

INTERVENTIONS: Students found guilty of committing any of the cases below after due process shall be subjected to immediate dropping or expulsion.

1. Intentional posting or sending messages that malign the reputation of the student or teacher or anyone that harms the whole organization
2. Creating harmful or malicious software
3. Using any social media platforms for illegal purposes
4. Hacking/ gaining of unauthorized data in a system or computer
5. Establishing networks or network connections to make live communication including audio and video without prior approval from the owner
6. Intentionally setting up or creating application that harms the software or hardware

NOTE: CODE OF CONDUCT AND POLICIES ON DISCIPLINE STATED IN THE STUDENT HANDBOOK STILL EXIST FOR SY 2020 - 2021

E. REMEDIAL ACTIONS and PENALTIES

Violators of this policy will be subject to the disciplinary procedure of the school and may result in the loss of access to the school domain. Violations of the policies described above for legal and ethical use of the school's IT system will be dealt with in a serious and appropriate manner. Suspensions means the student will not attend from online classes but Ed Tech will be informed. No deduction in the Conduct Grade.

Any determination of non-acceptable usage serious enough to require disconnection shall be promptly communicated to every representative of the school IT System member through an established means of publication. When EdTech learns of possible inappropriate use, ITS staff will notify the member responsible, which must take immediate remedial action and inform the Prefect of Students. In an emergency, in order to prevent further possible unauthorized activity, ITS may temporarily disconnect that member from the School IT System. If this is deemed necessary by ITS staff, every effort will be made to inform the member prior to disconnection, and every effort will be made to re-establish the connection as soon as it is mutually deemed safe.

**F. SECURITY**

The school IT System assumes that users are aware that electronic files are not necessarily secure. Users will be informed of methods available for protecting information from loss, tampering, unauthorized search, or other access. Levels of obtainable security will vary depending on the computer system. Please be aware of the potentially offensive material found in those archives and use the system with the recognition that the school IT System neither assumes responsibility for, nor endorses, any of the content found therein. Hence, the information contained in all emails and shared files, including those in its attachments, is confidential and intended only for the person(s) or entity(ies) to which it is addressed. If you are not an intended recipient, you must not read, copy, store, disclose, distribute this message, or act in reliance upon the information contained in it. It does not tolerate any unlawful, illegal, unauthorized, harassing and disruptive messages that violate our acceptable use policy.

Furthermore, the message is unmonitored and unsupervised, hence, any views expressed by the sender do not necessarily express or reflect the views and/or opinions of the school administration. If you received the email/file in error, please contact the sender and delete the material from any computer or system. You can also notify through the school official communication email.

G. CONFIDENTIALITY

In general, the school IT System will treat information stored on computers as confidential (whether or not that information is protected by the computer operating system). Requests for disclosure of information will be honored. Except when inappropriate, computer users will receive prior notice of such disclosures. (Viewing of information in the course of normal system maintenance does not constitute disclosure.)

## H. WARNING

Users of electronic mail systems should be aware that electronic mail in its present form cannot be secured and is, therefore, extremely vulnerable to unauthorized access and modification. Users must take caution in sending information via school internet access.

## I. ACCOUNT EXPIRATION

Access to the school IT System will be discontinued only if an old student is not officially enrolled within the current school year. For students who transfer, dropped and dismissed, his/her account is automatically suspended, and as for the graduates/ alumni they can still use their accounts but with limited access to e-learning platforms.

## J. DISCLAIMER

As part of the services available through the school IT System which provides access to a large number of conferences, lists, bulletin boards, and information servers. Some of these may contain objectionable material. For those facilities for which the school IT System has control, the policies described here apply. Thus, it takes no responsibility for the content of those entities over which it has no control.