Redland Christian Migrant Association (RCMA)

Internet Security and Safety Policy

I. Overview

RCMA supports instruction through the use of educational and administrative computers. The responsible use of computers and computer networks is a powerful tool in support of the instructional program. Some uses of computers and the Internet however possess no educational value in a school setting. This Internet security and safety policy serves to protect the interests of RCMA and technology resource users by outlining acceptable and unacceptable use of the network and computers used within RCMA.

It is a general policy that all RCMA computers be used in a responsible, efficient, ethical and legal manner. Failure to adhere to the policy and the guidelines for the use of RCMA computers as described in this policy could result in the revocation of access privileges and may result in appropriate disciplinary or legal action.

II. Terms and Conditions for Use of Computer and Network Resources

Authorized Users: Students and employees of RCMA who complete, sign, and return the Technology Resource User Agreement are authorized users of RCMA technology resources. All RCMA employees, students, and parents or legal guardians shall receive this agreement, and upon its return to the school, authorization shall be granted. The school system will maintain an accurate record of authorized users. Community and family members are authorized to use RCMA computers and network under supervision and/or guidance from RCMA employees or volunteers.

Electronic Mail: The RCMA email system is maintained and controlled by the Manage Information System (MIS) Team. MIS will provide email accounts to employees in fulfilling their duties and as an educational tool. Email is not private and may be monitored by MIS network administrators. Unauthorized access to email accounts by any student or employee is prohibited. Users shall be held personally liable for the content of any electronic message they create. Downloading any file attached to an electronic message is prohibited unless the user is certain of that message's authenticity and the nature of the file.

III. Acceptable Uses

A. Educational Purposes. RCMA is providing access to its computer and network for Internet access to support educational purposes. Acceptable use is defined as any computer activity in support of education and research, or the business of conducting education, consistent with the educational objectives of RCMA. Additionally, any RCMA user's traffic that traverses another organization's network or computing resources must comply with that network's Internet Security and Safety Policy. RCMA firmly believes that the educational value of the Internet far

outweighs the possibility that users may procure material that is not consistent with the educational goals of the school system.

B. Administrative and Operational Purpose: RCMA is providing access to its computer networks and the Internet for RCMA employees to complete administrative and operational tasks within RCMA.

C. Netiquette

The use of RCMA computer and network resources requires the user to abide by accepted rules of network etiquette. Netiquette is defined as being responsible for one's own actions and being respectful of others while using RCMA computer and network resources. RCMA reserves the right to judge and act upon questionable user activity on a case-by-case basis. All users must abide by rules of network etiquette, which include the following, the list is not inclusive:

- Be Polite: Use appropriate language. No swearing, vulgarities, suggestive, obscene, or threatening language.

- Do not send abusive messages to anyone: Do not send threatening, harassing, vulgar, obscene, or pornographic material is prohibited. Do not send abusive or hate messages to anyone or about anyone. This includes sending messages via email, instant messaging, chat rooms, or text messaging; posting messages in newsgroups, forums, or on the web;

- Do not write or contribute to abusive, derogatory and hate blogs. "Hate Crime" means (i) a criminal act committed against a person of his property with the specific intent of instilling fear or intimidation in the individual against whom the act is perpetrated because of race, religion or ethnic origin or that is committed for the purpose of restraining that person from exercising his rights under the Constitution or laws of this Commonwealth or of the United States, (ii) any illegal act directed against any persons or their property because of those persons' race, religion or national origin, and (iii) all other incidents, as determined by law-enforcement authorities, intended to intimidate or harass any individual or group because of race, religion or national origin.

- Avoid the use of language that may be offensive to others: Do not make or distribute jokes, stories, or other material that is based upon slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, or sexual orientation.

- Do not assume that a sender has given you permission to forward or redistribute their messages or personal information to others: Forwarding or redistributing a sender's email message or email address should not be done unless you know the sender would have no objection.

- Be considerate when sending email attachments: Be sure that the file is not too large to be accommodated by the recipient's system and that the file is in a format that the recipient can open.

- Do not send inappropriate or suggestive messages or images to anyone: Once it is gone, you cannot get it back, and although you may have intended it to be viewed by someone in confidence, such privacy is not guaranteed. An example of this type of behavior is called "sexting," which involves texting or emailing sexually-compromising messages or images.

IV. Unacceptable Uses of RCMA Computer and Network Resources

Unacceptable use is defined as any computer activity that does not support the educational and service mission of RCMA. Do not use RCMA computers for non-educational purposes. Examples of inappropriate activities include:

- Commercial activity by any individual or organization, regardless of for-profit or not-for-profit status;
- Product advertisement;
- Political lobbying;
- Actions relating to, or in support of, illegal activities. Illegal activity is defined as a violation of local, state, or federal laws;
- Sending or downloading copyrighted materials such as pictures, music, or movies;
- Plagiarism or the copying of documents, software, and other licensed materials protected by federal or state intellectual property of copyright laws;
- Use of email to forward chain letters or to send mass mailings that are not school or mission related;
- Viewing or transmitting pornography;
- "Hacking" and other unauthorized access to RCMA information or Internet resources;
- Uploading damaging materials such as worms, viruses, "Trojan horses," or other harmful or destructive forms of programming or software;
- Altering or causing harm to RCMA computer and network resources, such as the intentional corruption of operating systems, files, and network activity;
- Installation of software; and physical destruction or changes to configuration of hardware (computers, monitors, cables, mice, keyboards, printers, etc.);
- Downloading, transmitting, or storing inappropriate and/or large files such as digital images, graphics, movies, games, or digital music. Network capacity is limited;

V. Security

Security on any computer system is a high priority; the following items are applicable to ensure a secure environment for use of computers and the network:

- If users can identify a security problem, they must notify the teacher, school principal or MIS as soon as possible. Users must not demonstrate the problem to other users.

- Use of RCMA personally assigned accounts or passwords are not transferable and should not be shared.

- Any actions intended to compromise network security are prohibited.

- Any user identified as a security risk, or having a history of problems with other computer systems, may be denied access to RCMA computer and network resources.

- Use of Non-RCMA Technology Resources is only authorized once approved by the Information Technology Director. Use of personal devices are subject to monitoring and could have data seized for formal or informal investigations.

VI. Internet Filtering and Safety

RCMA will take all possible precautions to restrict access to undesirable materials on the Internet. Access of materials that may not be considered to be of educational or mission value in the context of the school or office setting is restricted. RCMA utilizes a combination of Websense, Mail Marshall and Sonic Walls to achieve this goal. Additionally, all network activity is monitored, and logs may be reviewed by network administrators periodically during normal system maintenance. Unfortunately, due to the dynamic nature and exploding growth of the Internet, not all undesirable material can be immediately or effectively blocked by RCMA's Internet blocking tools. On a global network it is impossible to control all materials, and an advanced net user may well be able to access controversial information. Users are expected to understand that it is their responsibility to use the Internet appropriately, and students, parents, and RCMA employees must work together to ensure the Internet is being used in a safe and appropriate manner. Students or employees who have gained access to, or have knowledge of another user's access to undesirable Internet materials must report this incident to their teacher, principal or supervisor. Parents and teachers who are aware of inappropriate sites should report the sites to the MIS team; the offensive sites will be restricted immediately.

A. General Warning – Individual Responsibility of Parents and Users

All users and their parents/guardians are advised that access to the Internet may include the potential for access to materials inappropriate for school-aged or pre-school children. Every user must take responsibility for his or her use of the Internet and stay away from inappropriate sites. As best as they are able, parents/guardians should attempt to stay abreast of the types of Internet activities their children engage in at school, home and away from school.

B. Personal Safety

Be safe. In using RCMA computers and network resources and the Internet, do not reveal personal information such as your full name, home address, telephone number, or other identifying information that might allow a person to locate you. Do not arrange a face-to-face meeting with someone you "meet" on the Internet without your parent's permission (if you are under 18). Regardless of your age, you should never agree to meet a person you have only communicated with on the Internet in a secluded place or in a private setting.

C. Confidentiality of Student Information

Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian or, if the student is 18 or over, the permission of the student. Users should never give out private or confidential information about themselves or others on the Internet, particularly credit card numbers or social security numbers. A supervising teacher or administrator may authorize the release of directory information, as defined by the RCMA Information Computer and Security Procedures, for internal administrative purposes or approved educational projects and activities.

D. In-Appropriate Communication

Sexting, the action of texting or emailing sexually-suggestive and personally compromising messages or images, will lead to nothing but problems for the sender. Once the "sext" is sent, the message that was intended to be privately shared can proliferate throughout the Internet without the sender's permission.

VII. Privacy

RCMA reserves the right to monitor, inspect, copy, review, and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information shall be and remain the property of RCMA and no user shall have any expectation of privacy regarding such materials.

VIII. Violations and Consequences

Use of RCMA computer and network resources is a privilege, not a right. Inappropriate use will result in an immediate termination of access and other privileges relating to use of RCMA resources. Any violation of these regulations may also result in appropriate disciplinary action (up to and including suspension or expulsion for students or formal reprimand or dismissal for employees) as well as potential civil or criminal liability and prosecution. Hate crimes (hate crimes are a criminal offense) and bullying by electronic means including blogs will be treated as seriously as traditional hate crimes and bullying. Off campus behavior can lead to escalating conflict that spills over to schools. Consequences will be given for hate crime cyber bullying and blogs that impact or disrupt any school related activities, functions and individuals.

IX. Liability

RCMA cannot guarantee the availability of technology resources. The MIS team cannot be held responsible for any information that may be lost, damaged, or unavailable due to technical or other difficulties. The MIS team cannot ensure that all electronic transmissions are secure and private; it depends on the user's methods and applications being used. The MIS Team cannot guarantee the accuracy or quality of information obtained. The MIS Team has made every effort to filter inappropriate material from access to RCMA users, but it cannot fully filter, control, or censor illegal, defamatory, or potentially offensive materials that may be available to the user on systems accessible through RCMA.

X. Internet Safety Program

The Internet provides students and employees with access to a wealth of information and educational resources along with the opportunity for collaboration with other students around the world. Unfortunately, it also offers access to inappropriate content and the opportunity for interaction with persons with intent to cause harm. RCMA believes that the benefits outweigh the disadvantages; however, it is critical that RCMA, parents/guardians, and employees work together to provide a safe environment and teach children ways to protect themselves while on the Internet. The Child Internet Protection Act (CIPA) requires schools and organizations receiving Erate funding (for the Internet) to integrate a component of Internet safety within the instructional program. In compliance with CIPA the Internet Safety Program includes:

1. **Professional Development**

- Training for staff
- Presentations for parents
- Instruction for students

2. **Filter for Internet access**

- Internet use is monitored by teachers at all grade levels.
- A review process is in place to consider exemptions or changes to the filter. The technology staff regularly reviews new and emerging technologies to see that they can be safely deployed and to make necessary changes in filtering and access.

3. **Security of data on RCMA network**

- No unfiltered access to the Internet is allowed.
- A firewall is in place to prevent inappropriate access to RCMA data and to protect children and students.

- Anti-spam and anti-virus software are in place.

- Network is monitored.

- Most student workstations are protected with software that prevents the changing of the computer configuration from its initial state.

- The technology staff has the ability to remotely monitor and access networked computers.

- The technology staff attempts to stay abreast of emerging technologies and implements new security measures as necessary.

- All critical data and applications that reside on the network are password and security rights protected.

4. **Roles and Responsibilities**

- **Teachers -** Be familiar with and report all claims of cyber bullying. Monitor student Internet and other technology use. Include Internet safety concepts in curriculum and when using technology with students. Be familiar with provisions of and monitor for violations of copyright and ethics standards as regards to the use of technology and the Internet.

- **Parents and Guardians -** Learn more about dangers that students may encounter while using the Internet. Monitor Internet and technology use by their children. Employ appropriate Internet filtering safeguards on home Internet devices.

- **Students -** Abide by guidelines set forth in the Acceptable Use Agreement.

- **Information Technology Director (IT Director) –** Properly execute and enforce computers and network security/safety requirements for use of technology resources. Be prepared to provide training assistance to charter schools and centers to meet RCMA requirements.

5. **Procedures to Address Breach of Security and/or Safety**

- All minor security and safety breaches are handled at the school level by school staff and center coordinators. Minor breaches might include students accessing inappropriate websites or teachers not logging off the computer and giving students access to their network accounts.
- All major security and safety issues are handled by the technology staff, Executive Director, IT Director, Charter Schools Director, and school principals. Major breaches are those that might include loss of service or data, or violation of local, state, or federal laws. Outside agencies and law enforcement may be involved if necessary.

- Documentation of security and safety breaches are maintained by the technology staff. If student discipline is involved, documentation is kept at the school level as well. If staff discipline is involved, documentation is kept in the staff member's file at the Human Resources office.

- It is of utmost importance that the IT Director ensures that any breaches are handled in accordance with the RCMA Information and Security Procedures.

6. **Design and Evaluation**

- RCMA will annually review, evaluate, and revise the Internet safety program as necessary.

- Each school will be accountable for providing information regarding the implementation and evaluation of lesson/activities.

- School Principals and the RCMA Education Director, in conjunction with IT Director will monitor new innovations in Internet safety and security services, professional development, and curricula.

Student Technology Responsibility Agreement

I understand and will abide by the above terms and conditions and acceptable uses of computers and networks provided by RCMA. As a student of RCMA, I agree to model appropriate netiquette and abide by the letter and spirit of acceptable use as defined in the policy. Additionally, I agree to report any misuse of computer and network resources to my teacher.

I understand that even though RCMA has an Internet filtering system, it is impossible to restrict access to all controversial materials. I will not hold RCMA responsible or legally liable for materials transmitted to or acquired by me from the network. Should I commit any violation, my access privileges may be revoked and school disciplinary action may be taken. I understand and will comply with Netiquette below, with the understanding that the list is not inclusive:

- Be Polite: Use appropriate language. No swearing, vulgarities, suggestive, obscene, or threatening language.
- Do not send abusive messages to anybody: Do not send threatening, harassing, hate, vulgar, obscene, or pornographic material. Do not send abusive or hate messages to anyone or about anyone. Do not write or contribute to abusive, derogatory and hate blogs.
- Avoid the use of language that may be offensive to others: Do not make or distribute jokes, stories, or other material that is based upon slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, or sexual orientation.
- Do not assume that a sender has given you permission to forward or redistribute their messages or personal information to others: Forwarding or redistributing a sender's email message or email address should not be done unless you know the sender would have no objection.
- Be considerate when sending email attachments: Be sure that the file is not too large to be accommodated by the recipient's system and that the file is in a format that the recipient can open.
- Do not send inappropriate or suggestive messages or images to anyone: Once it is gone, you cannot get it back, and although you may have intended it to be viewed by someone in confidence, such privacy is not guaranteed. An example of this type of behavior is called "sexting," which involves texting or emailing sexually-compromising messages or images.

_____

Print Name of Student Grade

_____

Signature of Student Date

Parent/Legal Guardian Technology Responsibility Agreement

As the parent or guardian of my student (s), child or children I have read the Terms and Conditions and Acceptable Uses of computers and networks provided by RCMA. I understand that this access is designed for educational purposes, and RCMA has taken available precautions to eliminate controversial materials. However, I also recognize it is impossible for RCMA to restrict access to all controversial materials, and I will not hold them responsible for materials available on the network. I understand and will help ensure my child/children understand Netiquette which is listed below; with the understanding the list is not inclusive:

- Be Polite: Use appropriate language. No swearing, vulgarities, suggestive, obscene, or threatening language.
- Do not send abusive messages to anybody: Do not send threatening, harassing, hate, vulgar, obscene, or pornographic material. Do not send abusive or hate messages to anyone or about anyone. Do not write or contribute to abusive, derogatory and hate blogs.
- Avoid the use of language that may be offensive to others: Do not make or distribute jokes, stories, or other material that is based upon slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, or sexual orientation.
- Do not assume that a sender has given you permission to forward or redistribute their messages or personal information to others: Forwarding or redistributing a sender's email message or email address should not be done unless you know the sender would have no objection.
- Be considerate when sending email attachments: Be sure that the file is not too large to be accommodated by the recipient's system and that the file is in a format that the recipient can open.
- Do not send inappropriate or suggestive messages or images to anyone: Once it is gone, you cannot get it back, and although you may have intended it to be viewed by someone in confidence, such privacy is not guaranteed. An example of this type of behavior is called "sexting," which involves texting or emailing sexually-compromising messages or images.

_____

Print Name of Parent or Guardian

_____

Signature of Parent or Guardian Date

RCMA Computer User Agreement (HR59)

RCMA encourages employees to use computer and technology resources, including the internet in creative and productive ways to support our mission of "opening doors to opportunities for children, families and staff." However, there are limitations on how these resources may be used in order to protect RCMA property and maintain RCMA's quality reputation.

RCMA, upon hire, enters into this agreement with each employee to ensure the appropriate use of technology as defined in this agreement.

General Guidelines

1. Proper electronic communication conduct should be used when communicating via e-mail or other electronic communications. Giving out personal information is inappropriate. When using e-mail, extreme caution must always be taken in revealing information of a personal nature.
2. The sharing of RCMA email and other systems passwords is prohibited.
3. Subscriptions to email lists that are for entertainment or unrelated to RCMA's mission are prohibited.
4. Limited personal use of the computer is allowable, i.e. checking child's homework assignments, brief checks of personal email accounts, appointment setting, etc. and should be done during breaks and non-work hours.

Unacceptable Use

1. Any use of the network for commercial or for-profit purposes is prohibited.
2. Hardware and/or software shall not be destroyed, modified, or abused in any way.
3. Hate mail, chain letters, harassment, discriminatory remarks, and other antisocial behaviors are prohibited on the network. This includes participation in pyramid or similar schemes.
4. Personal Instant Messaging or Personal Chats are prohibited.
5. The unauthorized installation of any software, including shareware and freeware, for use on RCMA computers is prohibited. Any software downloads must be approved by MIS.
6. Use of the network to access or process pornographic material or any inappropriate text files is prohibited.
7. The RCMA network may not be used for downloading entertainment software or other files not related to the mission and objectives of RCMA or for transfer to a user's home computer, personal computer, or other media. This prohibition pertains to freeware, shareware, copyrighted commercial and non-commercial software, and all other forms of software and files not directly related to the educational, instructional, administrative, and operational purposes of RCMA.
8. Use of profanity, obscenity, racist terms, or other language that may be offensive to any user is prohibited.

9. Playing games is prohibited unless specifically authorized by a teacher for instructional purposes. MIS will validate proper copyright and licensing regulations are being followed.
10. Employee family members, friends or other individuals not employed by RCMA are not authorized to use RCMA staff computers; they must only use computers specifically identified for general community use.
11. RCMA email accounts may not be used for personal reasons.
12. RCMA email accounts may not be used to send or forward material that could be considered as confidential, political, religious, obscene, threatening, offensive, or hateful.

Privacy

1. All computer, Internet, and e-mail systems supplied by RCMA are the property of RCMA and subject to control and monitoring at any time. This includes all hardware, software, messages, electronic correspondence and attachments sent over the RCMA network. RCMA employees should have no expectation of privacy in the use of RCMA computer systems.

I, _____, understand and agree to follow and obey the rules and regulations as outlined above and understand that failure to do so may have consequences that include disciplinary action up to and including immediate termination of employment with RCMA.

_____ _____

Signature Date

_____ _____

Supervisor Date