RANDOLPH CENTRAL SCHOOL CORPORATION
NETWORK AND INTERNET ACCEPTABLE USAGE
POLICY STUDENT AGREEMENT
Policy Approved on June 19, 2014

1.0 Overview
Access to computers and the Internet through the Randolph Central School Corporation computer network comes with the responsibility to use this network in a productive and ethical manner. Randolph Central School Corporation is in compliance with the Children's Internet Protection Act (CIPA) and has installed technology protection measures for all computers in the school corporation.

The Internet can contain information that may be judged as inaccurate, abusive, profane, sexual-oriented, or illegal. Randolph Central School Corporation does not condone or permit the use of this material. The use of technology within the school setting is a privilege, not a right, and it is a joint responsibility of school personnel and the parent or guardian of each student to educate the student about his or her responsibility when using the Internet.

Parents and guardians must be aware that while at school, direct supervision by school personnel of each student using the computers is not always possible. Thus, students are expected to use the resources in a manner consistent with this contract and will be held responsible for their use. Additionally, parents should discuss with their children their own expectations for their child's Internet use.

The corporation makes no guarantee that the functions or the services provided by or through the district network will be error-free or without defect. The district will not be responsible for any damage suffered, including but not limited to, loss of data or interruptions of service. The corporation is not responsible for the accuracy or quality of the information obtained through or stored on the network. The corporation will not be responsible for financial obligations arising through the unauthorized use of the network.

2.0 Purpose
The purpose of this policy is to outline the acceptable use of computer equipment at Randolph Central School Corporation. These rules are in place to protect the user and Randolph Central School Corporation. Inappropriate use exposes Randolph Central School Corporation to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope
This policy applies to students, teachers, substitutes, contractors, consultants, temporaries, and other persons at Randolph Central School Corporation , including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Randolph Central School Corporation.

4.0 Policy
4.1 General Use and Ownership
1. Users should be aware that the data they create on the corporate systems remains the property of Randolph Central School Corporation. Because of the need to protect Randolph Central School Corporation 's network, Randolph Central School Corporation does not and will not guarantee the confidentiality of information stored on any network device belonging to Randolph Central School Corporation .
2. For security and network maintenance purposes, authorized individuals within Randolph Central School Corporation may monitor equipment, systems and network traffic at any time, for any reason, without prior notice.
3. Randolph Central School Corporation reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information
1. All users, staff and students, are given an account upon their entry into the district. Any person to whom an account is given is the only person to use that account. Each user is responsible for the security of the system.
2. Passwords should not be shared. Authorized users are responsible for the security of their passwords and accounts. If a user shares a password with another, that user is as responsible for any ensuing action as the person actually performing the action, and will be held accountable.
3. System level and user level passwords may be changed as needed.
4. All PCs, laptops, iPads, and Chromebooks should be logged-off or locked when left unsupervised.
5. Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Users may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is a user of Randolph Central School Corporation authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Randolph Central School Corporation owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.4 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Randolph Central School Corporation
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Randolph Central School Corporation or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others.
6. Using a Randolph Central School Corporation computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any Randolph Central School Corporation account.
8. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
9. Port scanning or security scanning is expressly prohibited.
10. Executing any form of network monitoring which will intercept data not intended for the user.
11. Circumventing user authentication or security of any host, network or account.
12. Interfering with or denying service to any user (for example, denial of service attack).
13. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session.

4.5 Email and Communications Activities

1. Use of non-corporation issued email accounts is prohibited unless needed for an individual course, applying to a college or a similar circumstance that has been approved by the administration.
2. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
3. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
4. Unauthorized use, or forging, of email header information.
5. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
6. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type that involve money.

5.0 Enforcement

5.1 Student Rights

Students' right to free speech applies to communication on the Internet. Randolph Central School Corporation's electronic network is considered a limited forum, similar to the school newspaper, and therefore the district may restrict a student's speech for valid educational reasons.

5.2 Due Process

The district will cooperate with local, state, or federal officials in any investigation related to any illegal activities conducted through the district network.

In the event there is an allegation that a student has violated the district acceptable use policy, the student will be provided with a written notice of the alleged violation. An opportunity will be provided to present an explanation to an administrator.

Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic network. Violations of the acceptable use regulation and policy may result in a loss of access as well as other disciplinary or legal action.

If the violation also involves a violation of other provisions of other school rules, it will be handled in a manner described in the school rules. Additional restrictions may be placed on a student's use of his/her network account.

Any user found to have violated this policy may be subject to disciplinary action.