Technology Acceptable Use Policy (AUP) *and* Signature Page

NRC Technology Acceptable Use Policy

Introduction
The North River Collaborative understands the vital role that technology plays for both students and staff in education and is therefore committed to providing both hardware and software, as well as support for that purpose.

Collaborative Property
All aspects of the North River Collaborative's Technology Network (the "Network"), which includes computer, technology and communications systems, hardware, software and all message contents, Internet access, electronic mail capability, voice mail, and all uses of any stationary/cell telephonic equipment owned by the Collaborative are the property of the Collaborative. The Network is not a resource intended for use as a public forum or for any purpose that is not directly related to the delivery of educational services.

Expectation of Privacy
Use of the North River Collaborative's computers, Internet, and email are not private. At any time, and without prior notice, the North River Collaborative reserves the right to monitor, inspect, copy, review, and store any and all usage of technology devices.

Internet traffic may be monitored by the Collaborative at any time to ensure compliance. In addition, all incoming and outgoing emails are archived through our email host. Staff should not have any expectation of privacy regarding digital technology resources. An employee's access code or password does not give any right to privacy with respect to using the Collaborative's email, Internet, and voicemail systems.

The Collaborative assumes no responsibility for any unauthorized charges or fees; any financial obligations arising out of unauthorized use of the Network for purchase of products or services; any costs, liability, or damages caused by a user's violation of these policies; and any information or materials transferred through the Network.

User Responsibility
All staff must adhere to this acceptable use policy which includes both responsible use and prohibited use. Responsibility of use includes the day-to-day operation of technology, securing

or locking a device when not at the device, failing to log off the Network at the end of a work session or at the request of the system administrator, and failing to keep all passwords to the Network secure. All electronic contact should be through the North River Collaborative's email, website, and telephone system.

Employees should seek technical support for hardware or software problems via the NRC Help Desk. Tech support requests, through the technology staff directly or through email phone calls or texting, are not recommended as a valid form of seeking tech support and may not be responded to.

Users are expected to have a basic understanding of how to operate hardware and software.

Prohibited Uses of the Network

The Collaborative, in its sole discretion, can determine what a prohibited use of the Network is. If a user of the Network has any questions about the propriety of a particular use, then the user is cautioned to seek advice and consent from the technology department before the use occurs. Examples of prohibited uses include, but are not limited to:

- Engaging in unlawful or inappropriate behavior;
- Using the Network for financial gain or for any commercial, political, gambling, or any illegal activity;
- Transmitting/receiving material that contains offensive or harassing remarks based on race, color, national origin, religion, sex, disability, age, sexual orientation, military service, gender identity or expression, pregnancy and pregnancy-related medical conditions, or any other classification protected by law;
- Transmitting/receiving sexually explicit material, including messages, pictures, jokes, and cartoons;
- Accessing or visiting websites that contain sexually explicit, racist, or other offensive material or posting messages at these websites;
- Pirating software or downloading or transmitting/receiving software programs or any other copyrighted or trademarked materials;
- Identifying or sharing the location of inappropriate materials;
- Leaving one's computer logged in but unsecured or leaving password information available for others to assume your ID;
- Using the Network in any way which results in a potential claim concerning a copyright and/or trademark;
- Participating in any communications that facilitate the illegal sale or use of drugs or alcohol;
- Participating in any communications that facilitate criminal activity;
- Participating in any communications that threaten, intimidate, or harass any other person or violate any local, state, or federal laws;
- Attempting to access another person's files or any Network applications that the user does not have permission to be on;

- The use of proxy websites that allows a user to browse the Internet anonymously and intentionally bypasses NRC's firewall and content filters;
- Any form of vandalism, including damage to computers or hardware, and disseminating malicious software programs such as viruses that disrupt the operation of the Network;
- Disruption of Network/computer performance by changing configurations or attaching devices, physically or wirelessly to the Network;
- Using the Network on a personal device for any activities that are not work-related.

Violation of this Policy

The use of the Network is a privilege, not a right, which may be revoked at any time. Any violations of this policy may result in disciplinary action up to and including termination of employment. It should be further understood that transfer of certain kinds of materials is illegal and punishable by fine and/or jail sentence.

Classroom-Based Computer Use

The Collaborative's employees are responsible for ensuring that classroom-based computer use is in compliance with North River Collaborative and host school district policies regarding acceptable use and the Children's Internet Protection Act.

Internet Safety and CIPA Compliance

North River Collaborative through its ISP provides content filtering that is CIPA compliant. CIPA is the acronym for Children's Internet Protection Act. Our content filtering software is updated on a regular basis and sites can be blocked per our request. The software is in place to help protect our students from obscene or questionable material that is not educationally relevant.

The North River Collaborative will make every reasonable effort to monitor our Network, Internet traffic, and content filters to ensure student safety.

Disclaimer of Liability

While safeguards are in place to protect our staff and students from offensive material, no filter is 100% effective. The North River Collaborative disclaims all liability for the content of material that a staff member or student may access on the Internet, for any damages suffered in the course of or as a result of the Internet use, and any other consequences of staff member or student Network use. Under certain conditions, Massachusetts General Law (MGL) holds that email is public record and must be available for public inspection. North River Collaborative makes no guarantee, implied or otherwise, regarding the reliability of the data connection. The North River Collaborative shall not be liable for any loss or corruption of data resulting while using the Network.

Please sign the Acknowledgement Form on the last page.

Page intentionally left blank.

NRC Technology Acceptable Use Policy

Acknowledgement Form

I have read and understand all components of this **Technology AUP** document.

First and Last Name	(Print)
NRC Program	
Position	
Date completed	
Signature	