ROCHESTER COMMUNITY SCHOOLS
PRIDE IN EXCELLENCE

October 1, 2018

Dear RCS Families,

You may be hearing reports in the news about various data breaches that affected major companies across the country, such as Equifax, Yahoo, Facebook, and even Apple. We are living in unprecedented times, and school districts also remain a target for hacking.

Computer and technology use is a privilege in our schools, and all students are expected to behave responsibly. Late last year, a small number of students abused that privilege. School disciplinary sanctions were imposed, and the police are continuing their investigation.

When there is an ongoing police investigation, we cannot publicly share details that could have a negative impact on the investigation. We also trust that the community understands federal and state laws prohibit the district from publicly identifying the students or providing additional details concerning their actions. Such a disclosure may also unfairly prejudice the pending criminal proceedings. For these reasons, the district will not be making any future statements concerning this matter.

Student and staff safety and security is always our priority. The district is taking the necessary steps to confirm that none of our digital information has been altered, destroyed, or transferred. At this time, we are confident that our network and data are secure. However, we strongly encourage students to change their passwords on a regular basis and keep them safe. Staff members are required to change their passwords every 90 days and ensure their security.

Securing our network is a journey, not a destination. The threat landscape is continually evolving, but we remain diligent in our efforts to implement security measures to safeguard our data and our network.

Please take a moment to review the list of Frequently Asked Questions regarding the district's technology. If you have any questions or concerns, please feel free to call me at (248) 726-3100 or use the Talk to Us feature on our website at www.rochester.k12.mi.us.

Thank you for your continued support.

Sincerely,

Robert Shaner, Ph.D.
Superintendent

**TECHNOLOGY FREQUENTLY ASKED QUESTIONS**

The Rochester Community School District has identified technology and infrastructure as one of the three goal areas in the strategic plan so as to ensure all students are provided with a world-class education.

## 1. What are the district's strategic goals for information technology?

Strategic goals for information technology include:

- Creating sustainable, adaptable, and secure technology infrastructure
- Supporting technology needs of curriculum, instruction, and assessment
- Supporting collaborative, creative, and flexible learning environments with global access
- Supporting technology needs of staff
- Increasing learning opportunities for students
- Adhering to classroom technology standards
- Promoting device, technical, and professional development standardization
- Providing equal access to technology and promoting equity across classrooms, departments, programs, and schools

## 2. How is technology used to keep our students and staff safe in the buildings?

The district anticipates expending $6 million through the bond efforts to enhance student safety and school security. Efforts include redesigning the main building entrances with two sets of vestibule doors (along with a door to the office), and providing staff with a better visitor verification system and building lockdown capabilities. Locks that latch from the interior side of the classroom door are being added, and video surveillance cameras are being installed in the schools and on buses. An updated districtwide telephone system and Public Address (PA) system will also ensure proper notification and warning during an emergency.

## 3. What is the school doing to keep a child's digital information safe?

Securing a network is a journey, not a destination. The threat landscape is continually evolving, but we remain diligent in our efforts to implement security measures to safeguard our data and our network.

Through the bond efforts, we have been systemically replacing our aged infrastructure. This includes expanding our storage area network and virtual server environment and updating switches. We also added a robust wireless network and updated our firewall, content filter, and backup systems.

Other tactics to mitigate cybersecurity risks and safeguard our network and data include building awareness, encouraging employees and students to strengthen their passwords and keep them secure, and having restrictive permission policies. Additional tactics remain confidential to the organization so as to keep our network and student and staff information safe.

## 4. What is digital citizenship?

Digital citizenship involves developing the skills and knowledge for responsible technology use.

Our students start learning about digital citizenship as early as kindergarten. As students continue to learn and grow, age-appropriate material is introduced to ensure students learn about their digital footprint, how to use privacy settings to protect themselves, which online sources they can trust, ethical behavior, and how to apply their skills to pursue their passions.

## 5. How are student passwords managed?

The district recently purchased and installed new software so students in grades 5-12 can manage their own passwords. K-4 passwords are managed by the district to better support our youngest learners.

In order to prevent unauthorized access, the district strongly encourages all students to change their passwords regularly, ensure their strength, and keep them secure. Staff members are required to change their passwords every 90 days.

## 6. How can my son or daughter change their password?

Students in grades 5-12 can change their district and Google passwords by going to: https://rcspw.rochester.k12.mi.us/. (Students should allow 24 hours for Google to synchronize.)

Passwords must be a minimum of eight characters and contain both an upper and lower case letter and a number. The longer the password, the more secure it will be. The National Institute of Standards and Technology (NIST) suggests keeping passwords simple, long, and memorable by putting together a combination of words and numbers that only the user would know. To safeguard accounts, students should never use an RCS password on another site and never send, share, give, or make the password available to others.

## 7. How does the district deal with malicious activity involving cyber-threats?

At Rochester Community Schools, we take the safety of our students and staff very seriously. Protecting our family is always our top priority.

The district works with local law enforcement to investigate all threats. As such, we are prepared to prosecute to the fullest extent of the law anyone associated with dangerous and malicious activities, including those associated cybersecurity breaches. When there is an ongoing criminal investigation, we cannot publicly share details that could have a negative impact on the investigation.

For students: Computer and technology use is a privilege, and all students are expected to behave responsibly. In the Student Code of Conduct, the Board of Education established categories of misconduct, which may result in suspension or expulsion from Rochester Community Schools. These categories are descriptive of the most obvious types of misconduct and are not to be construed as an exclusive list or limitation upon the authority of school officials to address any other types of conduct which interfere with the proper functioning of the educational process. These categories also apply to infractions committed in a prior school/district.

Regarding electronic tampering, the Student Code of Conduct infractions include any unauthorized use, misuse or access of any of the school district's electronic equipment including, but not limited to, voice and video equipment, computers or use of the internet. Reference will be made to the Rochester Community Schools Acceptable Technology Use Agreement and classroom rules which may apply in cases of this misconduct. For all levels, restitution and repair or replacement of damaged property, and/or removal of computer privileges and possible loss of credit for the course may result.

## 8. What can parents do to help?

Keeping our children safe is a shared responsibility. According to the Michigan State Police, "parents should educate their children to be cyber smart. Prevention and awareness is the key to deter cyber predators and exposure to inappropriate material."

Discussion points may include the following:

- Only talk to people you know.
- Be a good digital citizen.
- Cyber-crimes are a violation of the student code of conduct, technology use agreement, and the law.
- Use your own district credentials to access the network.
- Report any suspicious activity to a trusted adult.

## 9. What are some resources for parents that can be helpful in the discussion?

Commonsense.org has produced a short video that can help guide a discussion with an elementary student. To view the video, go to: https://d1pmarobgdhgjx.cloudfront.net/education/ED_DigCit_MyOnlineNeighborhood.mp4.

The Oakland County Sheriff's Office has provided useful information, along with a podcast with Sheriff Michael Bouchard, for parents regarding internet safety at: https://www.oakgov.com/sheriff/Community%20Services/domestic/Pages/Internet-Use-Safety.aspx.