Table of Contents

Using this Handbook
User Agreements (EHB-AP1)
  Student Users
  Employee Users
  External Users
Getting Connected
  Login Checklist
  Login Types
  Raytown Technology WIKI
  Password Security
Email
  Responsibility
  Basics
  Signature Required
  Emailing Parents
    SISK12
    Email
Legal
Social Media
Digital Resources
  Learning Management Systems
District Devices
  Care of Devices
  Reporting Damage, Viruses, and Other Trouble
    Viruses and Malware
Loaner Devices
End of Year Process
  Computer
  Other Technology

updated 11/2022
Hardware Request
Guest Wireless
Get Technical Help
Phones and Voicemail
Updating Information in Technology
  Name
  Photo
Printing and Copying
SISK12
Training and Policy Review Video
Google Apps for Education
SISFIN
Safety
  Spam
  Phishing
Tips
Securing Data at Rest & Transit
What You Need to Know Now
Exceptions
Using this Handbook

This handbook is a guide to proper usage of technology by all employees of Raytown Quality Schools. You will be asked to sign an agreement stating you have read and understand this handbook and all associated policies and guidelines.

Digital copies of this handbook and all referenced documents are available on the staff section of www.raytownschools.org with working links to referenced documents and a navigable table of contents.

User Agreements (EHB-AP1)

All users must read and understand the General Rules and Responsibilities section of Board Policy EHB-AP(1), which pertain to usage and security.

Student Users

Users will be granted access privileges to district technology resources as determined appropriate by the superintendent or designee. Any attempt to secure a higher level of privilege without authorization is prohibited.

Employee Users

No employee will be given access to the district’s technology resources unless the employee agrees to follow the district’s User Agreement prior to accessing or using the district’s technology resources. Authorized employees may use the district’s technology resources for reasonable, incidental personal purposes as long as the use does not violate any provision of district policies or procedures, hinder the use of the district’s technology resources for the benefit of its students or waste district resources. Any use that jeopardizes the safety, security or usefulness of the district’s technology resources or interferes with the effective and professional performance of the employee’s job is considered unreasonable. Unless authorized by the employee’s supervisor in advance, employees may not access, view, display, store, print or disseminate information using district technology resources that students or other users could not access, view, display, store, print or disseminate.

External Users

Consultants, legal counsel, independent contractors and other persons having business with the district may be granted user privileges at the discretion of the superintendent or designee after consenting to the district’s User Agreement and for the sole, limited purpose
of conducting business with the school. External users must abide by all laws, district policies and procedures.

Getting Connected

On your first day you should receive your computer or be directed to a computer to use to check your access to essential applications. Some applications are used by all staff, while others are only used by specific groups. Below is a list of commonly used applications.

Note: The login ID used to access Raytown School District resources will depend on how the application is managed. There are two primary login IDs used by most systems, the first is your email address which is your firstname.lastname@raytownschools.org, and the second is what is referred to as your short login, which is typically your last name followed by your first initial.

The below chart lists frequently used systems along with how to log into each system. It is recommended that all new staff work through this list to ensure they can access the essential systems. Ask your administrator/supervisor or mentor which of these systems you should log in to.

Login Checklist

Login Types

<table>
<thead>
<tr>
<th>Login Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short Login</td>
<td>This is typically your last name first initial</td>
</tr>
<tr>
<td>District Email</td>
<td><a href="mailto:firstname.lastname@raytownschools.org">firstname.lastname@raytownschools.org</a></td>
</tr>
<tr>
<td>User Created</td>
<td>You have created this login</td>
</tr>
<tr>
<td>Static District Login</td>
<td>This is created by technology</td>
</tr>
<tr>
<td>Google</td>
<td>District email account</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System</th>
<th>Description</th>
<th>Login Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>District Computer</td>
<td>Must log in and set new password first before most other applications will work</td>
<td>District email</td>
</tr>
<tr>
<td>(not a chromebook)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Staff Intranet</td>
<td>Staff section of Raytown's district website</td>
<td>Short Login</td>
</tr>
</tbody>
</table>

updated 11/2022
<table>
<thead>
<tr>
<th>System</th>
<th>Description</th>
<th>Login Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email (Gmail)</td>
<td>Primary district communication</td>
<td>Google</td>
</tr>
<tr>
<td>SiSFin Employee Portal</td>
<td>Track pay and update personal information with HR and Payroll</td>
<td></td>
</tr>
<tr>
<td>TalentEd</td>
<td>Sign contracts, letters of reasonable assurance, certificated evaluations and professional growth plans</td>
<td></td>
</tr>
<tr>
<td>Frontline</td>
<td>Report absences Clock in and Out, Track Leave Balances</td>
<td></td>
</tr>
<tr>
<td>Brightly Helpdesk (Technology Service Requests)</td>
<td>Track technology service requests</td>
<td></td>
</tr>
<tr>
<td>Securly</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SISK12</td>
<td>Student Information System</td>
<td></td>
</tr>
<tr>
<td>SISK12 Pulse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clever</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Droplet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Requests &amp; Work Orders</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Raytown Technology Wiki**

The technology office maintains an updated help site, known as the “wiki” that will guide you through logging in to a majority of the systems used in the Raytown School District. To access the wiki, go to [https://wiki.raytownschools.org](https://wiki.raytownschools.org). The first time you visit the site, you will need to log in, by clicking the person in the upper right corner. You will use your provided user name and password.

**Password Security**

Passwords must be “strong” and are only reset in the event of a security incident. You cannot use your last 3 passwords and it must not be similar to your username.

**Strong Passwords**

- At least sixteen (16) characters in length.
- Must contain at least 3 of the 4 options below:
  - At least one (1) uppercase letter.
Email

The district uses Google Apps for EDU for email, document storage and collaboration. Although you can log-in through Google and your email looks very similar to a regular Gmail account, your District email is owned and managed by the district and is not a personal Gmail account.

Responsibility

Unless otherwise specified by your supervisor, you are expected to read and respond to email in a professional and timely manner. Email is a primary method of communication in and among district buildings and failing to check your email on a regular basis can leave you unaware of critical information.

A user is responsible for all email originating from the user’s email account.

1. Forgery or attempted forgery of electronic messages is illegal and prohibited.
2. Unauthorized attempts to read, delete, copy or modify electronic messages of other users are prohibited.
3. Users are prohibited from sending unsolicited mass email or other electronic messages, unless the communication is a necessary, employment-related function or an authorized publication.
4. When communicating electronically, all users must comply with district policies, regulations and procedures and adhere to the same standards expected in the classroom.
5. Users must obtain permission from the superintendent or designee before sending any districtwide electronic messages.

Basics

1. Log in to Gmail with these instructions available on our wiki site.
2. Always check the sender of an email message. Do not open messages from an unrecognized sender.
3. Never send passwords or reply to messages asking for your password. The district will never ask for your password through email.
4. Don’t use backgrounds in your messages and use easily legible fonts and limited colors.
5. Do not include quotes/sayings or images/logos as part of your email signature or template.
6. Do not include a student or staff name in the subject of your email. Anyone who can view your screen can easily see this information.
7. Find advanced Gmail help and more on the Technology Department’s WIKI site.
8. Email is to be used only for district business.

updated 11/2022
Signature Required

You are required to use the district standard email signature containing your name, position within the district, building, address, phone number (cell phone is optional), and email address. The title block will be in 11 point Calibri while the confidentiality statements will be in 9 point Calibri as in the example below. **Do not** use a scanned copy of your written signature and building mascots, logos or other images/quotes are not allowed within your signature.

Expect the Exceptional

Confidentiality notice for Raytown C-2 school district. This correspondence and any attachments are for the sole use of the intended recipient(s) and may contain confidential or privileged information. Any unauthorized use, disclosure, or distribution is prohibited and may be unlawful. If you are not the intended recipient or a person responsible for delivering this message to the intended recipient(s), please contact the sender and destroy all copies of the original message.

Emailing Parents

Parents can be emailed through SISK12 or District email. You must never include multiple parent email addresses in the TO: or CC: lines which will reveal email addresses to other parents.

SISK12

For most staff members you can follow the  Parents - Sending Email instructions located on our wiki tech support site. If you are a classroom teacher, you will need to follow these instructions. An individual email will be sent to each recipient and it will appear to come from your email address.

Email

- Email an individual parent directly from your district email.
- Email multiple parents by only using the BCC (blind carbon copy) line. No recipients will see the addresses of any other recipient.

Legal

Email messages are deleted after 14 months with no exceptions.

Emails may be printed on paper to keep past this time. Messages may not be stored in any digital format to surpass this limit. The technology department suggests that important
information such as schedules, lists, or instructions be stored in a separate Google document that does not contain the entire body of the email. Printed documents that may contain PII, or data protected under FERPA, HIPPA or COPPA should not be left on a printer, or a desk for all to see.

Social Media

The district encourages staff to use district-approved electronic media to communicate with parents and students; however, the line between public/private and personal/professional is blurred in the digital world. Unprofessional and/or inappropriate use of electronic media reflects poorly on the district as well as the individual and can be cause for disciplinary action.

Read and be familiar with board policy EHB-AP(3), Guidelines for All Electronic Media.
Digital Resources

The district provides many digital resources for use in the classroom. Visit the Software page on the staff intranet for a list of available resources. New resources are approved through a Software Request Form available on the staff intranet and are scrutinized under the Family Educational Rights and Privacy Act and Children’s Online Privacy Protection Act rules outlined in the chart below.

Teacher Software / Online Resource Use

1. Is the content safe for student viewing?
   - Yes
   - No, Stop - resource not allowed.

2. Does it directly align with the district curricular goal?
   - Yes
   - No, Stop - resource not allowed.
   - Yes

3. Is there a cost associated?
   - Yes
   - Does it have approval from curriculum coordinator?
     - Yes
     - Submit software request with budget code.
     - No
   - No

4. If free, does the free version meet my needs?
   - Yes
   - Does it collect or track student information?
     - Yes
     - Use district email account.
     - No
   - No

5. Does it require a teacher login?
   - Yes
   - Use district email account.
   - No

updated 11/2022
Learning Management Systems

A learning management system (LMS) is a software application for the administration, documentation, tracking, reporting, and delivery of electronic educational technology.

Several major systems will likely be included in your curriculum, with instructions on how they are to be used. Links to most LMS's are located on the staff intranet.

Google Classroom is the district’s adopted classroom LMS. Use of any other LMS not linked from the district Intranet is not allowed.

District Devices

The district issues devices to staff and students based on job role and instructional need. No devices will be issued before the district has the appropriate signed user agreements on file. Use of district devices must comply with all other technology policies. Device inventory and issuance is tracked by the technology department.

Care of Devices

The district expects those who receive devices to take reasonable precautions to prevent damage. Employees may be required to reimburse the district for any damage or theft that was the result of the employee's negligence.

- Use a case for cell phones and tablets.
- Transport laptops in provided carrying bags.
- When not using a laptop bag, carry it closed and with both hands.
- Any accidental damage must be reported immediately. Damage not reported immediately will be considered improper care of equipment and may be deemed negligence.

District devices may not be personalized in any way that is not immediately removable or has the potential to leave behind glue or other material.

- No stickers, paint, white out, ink, tape, glue, glitter, rhinestones, etc.
- Personal cases, covers, or bags are ok and may be personalized if not provided by the district.
Reporting Damage, Viruses, and Other Trouble

Damage to district devices should be reported to the technology office immediately. Students can report damage to their device, by submitting the Student Device Incident Form. Staff should report damage to their device, by submitting a service request.

Viruses and Malware

If you suspect your device has been infected by a virus or other malicious software, immediately contact the technology help desk at 816-268-7120.

Loaner Devices

Loaner devices can be given while regular devices are being repaired or replaced.

End of Year Process

Computer

- A sign out sheet is required and part of your paperwork to be signed off by your building administrator before leaving on break.
- Returning employees issued laptops will take the device with them over break.

Other Technology

All other technology used or checked out to you will need to be inspected or turned in before leaving. This technology is issued by classroom, not teacher, and includes but is not limited to:

- SMARTBoard & accessories
- Document cameras
- Cables to connect equipment
- Projectors
- Monitors
- Webcams
- Desk phones

Hardware Request

All technology purchases must go through the district technology department. If you or your building/department would like to add technology devices, you must submit a hardware request form. Hardware requests must be approved by a building principal, department administrator,
coordinator, or instructional coach. Fill out the form and follow the detailed instructions on page two.

**Hardware Request Form**

**Guest Wireless**
Guests bringing their own laptops or devices will need to request wireless access from the technology department. Guest Wireless should be requested at a minimum of 5 days before your event.

**Guest Wireless Form**

**Get Technical Help**

[Entering in a service request](#) is your first option to notify technology for help. This [wiki article](#) will assist you with submitting a service request. You can use the [problem type](#) description to get your issue to the correct person as quickly as possible.

You may also contact the Technology Helpdesk at ext. 7120 if you are unable to complete a request or cannot get in touch with your building tech.

**Phones and Voicemail**

The term “telephone system” is defined to include all telephones and voice mail messaging systems provided by the district to employees, students and patrons for their use. Access to the district’s telephone system is a privilege, not a right. Students and patrons may only use the district telephone system with appropriate authorization and supervision by a district employee.

You are responsible for reading and understanding the Telephone Rules section of [Board Policy EHB-AP(1)](#).

Classroom telephones will be operational for both incoming and outgoing calls during all non-class hours. During class hours, incoming calls will be answered by the building secretary and forwarded to the classroom teacher’s voice mail or to the classroom in cases of emergency. The building principal will designate specific district telephones that may be operated for both incoming and outgoing calls at any time during the class day (such as the counselor’s’ office, nurse’s office, departmental offices, etc.) and the administration will notify all employees of the location of these designated phones.

updated 11/2022
Updating Information in Technology

Name
Log into the Tyler SISFIN employee portal and click Submit Personal Info Changes. Once submitted, HR will review the changes and pass them to the technology department to update email and other systems.

Photo
Contact HR about updating your photo on your badge and in SISK12. To change your photo in Google, visit the Google page on the technology wiki site.

Printing and Copying
Staff are given access to printers in their building. All printers are deployed automatically based on your building. The instructions below will walk you through how to check your printers. If you are an Instructional Assistant, you will need to follow the Chromebook Printing section. If you do not have access to a specific printer, please enter a technology service request.

- Click on ^ in the lower right hand corner of the task bar.
- Right mouse click on the printer icon that is displayed
- Choose “View My Printers” or “Refresh My Printers”
  - “View My Printers” will open a window and give you a list of all of the printers that have been identified in your building.
    - You will see three “Follow Me” printers (you can send documents to print to any of these and go to any copier to release them.
    - Next to the name of each printer, you should see the word “Installed”. This means that the printer driver has been installed on your computer, and is ready to use. If you see anything other than “Installed”, please enter a Technology service request.

- Printing from Chromebooks:
  - Printing from a Chromebook is only configured for staff who are directly assigned a Chromebook as their primary work device.
  - Please install the following Chrome app on your Chromebooks: Mobility Print. Once the app is installed, you should have the ability to print to the "Follow Me" queue from your Chromebook.
  - The first time you print, on the print screen, select the drop down for the Destination and choose "see more...", and then select the Follow Me Secondary printer.
  - It will prompt you to sign in with your username and password (this is the computer username - lastnameofinitial, not your email). Then you can release the print job at the copier using the same login or your access card. If you have any questions or issues with this, please submit a Technology Service Request.
SISK12

SISK12 is the Student Information System K-12 used by Raytown to track all student data such as grades, attendance, and contact information. All teachers and school office staff and many other roles are required to use SISK12 regularly.

The SISK12 team in the Technology Department will provide appropriate training, electronic documentation through the SISK12 Help Site, and best practices. Student data policy and procedure is set by district and building administrators.

Training and Policy Review Video

In accordance with district practice, all staff must acknowledge viewing the technology policy video. This video is distributed annually to all staff through TalentEd Records in their Annual Review of Board Policy.

Google Apps for Education

The district has adopted Google Apps for Education to give staff and students access to Google's world class email, file storage, and collaboration tools. Training will be provided for new staff by the technology department as well as ongoing opportunities to learn advanced methods of interacting with students and other staff. The Technology wiki site provides tutorials on getting started and intermediate and advanced topics.

SISFIN

You will log in to SISFIN to view your pay stub and check your leave balance. It is available on the staff intranet page. Your default username is your last name and your password is your five digit employee ID.

Safety

Curricular or non-curricular publications distributed using district technology will comply with the law and Board policies on confidentiality. All district employees will abide by state and federal law, Board policies, and district rules when using district technology resources to communicate information about personally identifiable students. Employees will take precautions to prevent negligent disclosure of student information or student records.

All students will be instructed on the dangers of sharing personal information about themselves or others over the Internet and are prohibited from sharing such information unless authorized by the district. Student users shall not agree to meet with someone they have met online without parental approval and must promptly disclose to a teacher or another district employee any message the user receives that is inappropriate or makes the user feel uncomfortable.

updated 11/2022
Spam
Spam is a general term for any unwanted email whether it is an advertisement or a malicious email. Always check the email sender and verify you should be receiving an email from the sender before clicking links or responding.

Luckily, Google has several tools to mark spam emails to help filter spam emails. To mark an email spam select the email and at the top select the icon to mark as spam.

You can also select the drop down arrow next to the reply button within the email preview and select Report spam. You may also be more specific and select Report phishing if you wish.

Phishing
Phishing is an attack that attempts to steal your money, or your identity, by getting you to reveal personal information -- such as credit card numbers, bank information or passwords. Cyber criminals typically pretend to be reputable companies, colleagues, friends or acquaintances in a fake message. If you feel you have received a phishing email, please contact the Raytown Cyber Security team. Below are some common ways to identify a Phish:

- **Urgent call to action or threats** - Be suspicious of emails that claim you must click, call or open an attachment immediately.
- **First time or infrequent contacts** - When you get an email or call from somebody you don’t recognize, take a moment to examine it extra carefully before you proceed.
- **Spelling and bad grammar** - If an email message has obvious spelling or grammatical errors it might be a scam.
- **Generic greetings** - If the email starts with a generic “Dear sir or madam” that’s a warning sign that it might not really be your bank or shopping site.

updated 11/2022
● **Mismatched email domains** - If the email claims to be from a reputable company, like your bank, but the email is being sent from another email domain like gmail.com it's probably a scam. Be watchful for misspellings of the name, like micros0ft.com where the second “o” has been replaced by a 0 (zero).

● **Suspicious links or unexpected attachments** - Don’t open any links or attachments that you see, instead, hover your mouse over, but don’t click the link to see if the address matches the link that was typed in the message.

● **You did not initiate the conversation** - An often-used hook is to inform the recipient he or she has won a prize, will qualify for a prize if they reply to the email, or will benefit from a discount by clicking on a link or opening an attachment.

● **Request for credentials, payment information or other personal details** - One of the most sophisticated types of phishing emails is when an attacker has created a fake landing page that recipients are directed to by a link in an official looking email. The fake landing page will have a login box or request that a payment is made to resolve an outstanding issue. If the email was unexpected, recipients should visit the website from which the email has supposedly come by typing in the URL – rather than clicking on a link – to avoid entering their login credentials of the fake site or making a payment to the attacker.

**Tips**

Review the list of [online safety tips](#) available on the wiki site to avoid having personal data stolen and used against you.

**Securing Data at Rest & Transit**

All staff and students that log into a district issued computer will be provided with several options for data storage and transmission. Staff and students will need to ensure that they are securely storing their data. Staff and students will be able to store data on their local device. It is important to note that this data is not a part of the district’s continuity plan, and thus will not be backed up by the district’s backup solution. Staff and students may also have mapped personal and shared folders. These folders map to district file servers. Access to these files is restricted to the folder’s owner (staff or student who is assigned) and district enterprise administrator accounts.

Google drive is the district’s preferred location for your document storage. Google allows for infinite space for our employees to utilize in storing their files. Please be aware that all information is stored on Google’s servers and not locally, so if Google Drive is down, files will be inaccessible. As part of the software installed on your district device, the Google Drive desktop application should be set up to synchronize any files on your computer hard drive to a folder on your google drive. Files synchronized with this application will give you a G: drive and can be accessed from there. Files uploaded into a shared folder are accessible by all users who have

updated 11/2022
access to that folder by default. Check sharing settings on files and folders by clicking the blue share button. It is your responsibility to report any Google Drive or cloud storage security problems immediately. These can be reported by calling the Technology Helpdesk at ext. 7120.

Google Drive is also ideal for collaboration. Google makes it very easy to share and work on files simultaneously.

External Storage

The term “External Storage Devices” is used to define all portable storage devices (including USB drives, rewritable CD/DVD, memory cards, and external hard drives) used by staff and students. While the district recognizes the advantages for staff and students to maintain information on these devices, users are strongly encouraged to rely on their district provided Google Apps for Education Drive account for all storage needs.

When using external storage devices, staff must adhere to the following guidelines:

- Users are responsible for all content on external storage devices that have been connected to district technology resources.
- Users must ensure that they will not introduce harmful software including computer viruses, malware, non-district approved software, or hacking tools to district technology resources.
- Users must ensure that the data will remain secure through appropriate encryption or password protection when transferring files containing PII or protected information to an external storage device.
- Users should only keep the information stored on the external device for the duration of the project, and then promptly remove it.
- Staff should never transfer any documents labeled classified, confidential, or restricted to any external storage device.
- Staff should never transfer or create confidential data or student records on personal storage devices.
- When staff leave the district, they must ensure that they delete any district created/provided curricular or operational documentation, files, or data from their personal external storage devices.

Transferring Files

Policies and guidelines related to file storage apply to files in transit as well. It is your responsibility to secure sensitive data for transmission with encryption or a password. Classified, confidential, or restricted information should not be transferred through email, Google Drive, external storage devices, or third party file transfer services. See the Email and Safety sections for guidelines on safe email usage.

The district has the following guidelines in place regarding the transmission of data:

updated 11/2022
Staff are responsible for securing sensitive data for transmission through email or other channels with encryption or a password.

Staff should never include a password in any communication with the actual file attached that is being protected by the password.

Staff should never transmit files labeled classified, confidential, or restricted through email or third party.

Regular transmission of student data to services such as a learning management system is managed by the technology department using a secure data transfer protocol. All such services are approved by a district/building administrator and the Chief Information Officer.

The technology department can set up secure file transmission when needed. You must have the ISO’s approval for transferring data to other company’s Examples include approved software or websites that regularly need to receive and send student data. See the Digital Resources section for instructions to review and request use of software or a website.

What You Need to Know Now

1. Log in to your computer, raytownschools.org, and GMail.
2. Check your email every day.
3. Find the name of your building tech and remember the help desk extension of 7120.

Exceptions

Exceptions to district rules will be made for district employees or agents conducting an investigation of a use that potentially violates the law, district policies or procedures. Exceptions will also be made for technology administrators who need access to district technology resources to maintain the district’s resources or examine and delete data stored on district computers as allowed by the district’s retention policy.