RICHLAND ONE

Information Technology

Standard Operating Procedures

Updated 09.26.2024

Updates are noted in purple.

RICHLAND ONE

Table of Contents

Accessing YouTube and Google Chrome Extensions

Updated: May 7, 2024

A. **Accessing YouTube**

- YouTube is **not** blocked for students and staff; however, they are required to sign in with their District credentials.
- Check to make sure students can access the video by signing into YouTube using your District credentials.
  - Go to the video, and you will see an "approve" button under the video.
  - To the left of the approve button, there is a message that says, "This video is approved for Richland One" or "This video is not approved for Richland One."
  - Clicking approve will make the video available for all Richland One students.
- For additional instructions, see the video linked below.
  - YouTube Approval

B. **Approval of Chrome Extensions**

- Staff may submit a One to One Plus ticket and select “Chrome Extensions” as the ticket type to request an extension to be reviewed to be installed.
  - Information regarding the purpose and use of the extension must be included in the ticket. Tickets without this information will be closed.
- Once the extension has been vetted as not containing malware or other threats to district systems, the extension will be granted an exemption.

RICHLAND ONE

Approved Hardware Items
and
Pre-Approved Technology
Updated: February 22, 2023

Pre-approved technology ensures that all schools and departments purchase district-approved technology that is compatible with Richland One's network without going through the DRAPE process. This also helps them identify the best technology solutions by:

- Standardizing Technology Resources
- Identifying the latest and greatest technologies
- Providing costs to assist with project planning
- Eliminating redundant purchases
- Accommodating security and safety protocols

The Information Technology Department will provide an updated list of approved technologies supported on our network. The list will include technologies such as desktops, laptops, tablets, iPads, printers, interactive displays, LCD displays, and charging carts. This list will be updated periodically as vendors and manufacturers notify us of discontinuations and model upgrades.

See Pre-Approved Hardware Website

RICHLAND ONE

Blocking and Unblocking Websites

Updated: April 22, 2024

Initiation

To request the blocking or unblocking of a website, the requestor should submit a ticket through the District's Technology Help Desk Ticketing System (One to One Plus). The ticket type should be listed as "Web Filtering" so that it is routed correctly.

Please note that any website that requires you to create accounts for student learning is not considered requesting a website to be unblocked but is in fact a request to use an instructional program which must be reviewed by Teaching and Learning and vetted through the DRAPE process. Tickets for these requests will be closed, and you must submit a DRAPE for approval.

Approval

Upon ticket creation, Web Filtering tickets are routed to the Library Media Consultant in the Learning Environments and Instructional Resources (LEIR). Upon review of the website for instructional content and appropriateness by a group selected by T&L, the Library Media Consultant will note in the ticket whether the request is approved or not in the ticket notes and assign the ticket to the Network Security Manager in Information Technology (IT).

Blocking/Unblocking

Upon receipt of the ticket from the Library Media Consultant, the Network Security will block or unblock the site based on the findings from the evaluation and the recommendation of the Library Media Consultant. Once completed, the Network Security Manager will place a note in the ticket for the requestor and close the ticket.

RICHLAND ONE

District-Issued Cellular Phones

Updated: May 2, 2024

The Richland One Administration recognizes that cellular phones may be an appropriate communication tool for the efficient and effective operation of the District and to help ensure safety and security during the school day and at school-sponsored events and activities. To that end, the Administration authorizes the lease of cellular phones for employee use, as defined in this document.

Usage of Cellular Phones

District-Issued Cellular phones are provided to assist in the management of District business and ensure safety and security.

Employees issued a district-issued cellular phone are responsible for its safekeeping at all times. Defective, lost, or stolen district-issued cellular phones are to be reported immediately to the Telecommunications Specialist in IT, who will notify the service provider and arrange for a replacement district-issued cellular phone. Lost, Damaged and Stolen District-Issued Cellular phones must follow the districts TVLD process and all forms must be completed. Forms can be found on the Property Forms website.

District-Issued Cellular phones should not be used while driving either a District-owned vehicle or a personal vehicle used for District business.

District-issued cellular phones are provided for Richland One business only. No personal information should ever be stored on these devices. This includes, but is not limited to, photos, videos, messages, notes, email accounts, or personal applications.

District business is to be conducted on a district-issued cellular phone and not a personal cellular phone.

Staff are to always connect their district-issued cellular phone to the R1_StaffLink Wi-Fi network. Staff are to follow the directions outlined on the Network Access for District-Issued iPhones document for connecting to this network.

District-Issued Cellular Phone Repairs

Any repairs to district-issued cellular phones must begin with the creation of a One to One Plus ticket. Users must select "Cell Phones" as the ticket type and provide detailed information in the description of the ticket, to include, but not limited to the person's cell phone number, position, location, specific information as to the issue with the phone. The district technician will provide information in notes' section regarding next steps.

Repairs requiring parts or services from an authorized outside repair contractor will necessitate a school or department budget code to fund the repairs. The site's budget code must be provided in the notes' section of the ticket before the repair process can move forward.

Department supervisors must be informed of any required work on cellular devices if funding is necessary and must be added as a Collaborator on the One to One Plus ticket. Processing of the repair will not move forward until they are added by the user.

While minor repairs can often be completed onsite or within three business days in-house, more complicated repairs or service activations requiring assistance from outside providers may take three or more weeks due to parts sourcing and delivery logistics. During repair or service activation periods, the IT Department recommends notifying subordinates, coworkers, and vendors to utilize alternative means of communication until repairs or activations are completed. The district does not have loaner cellular phones that can be provided to staff.

Services requiring assistance from AT&T must be initiated before 1:00pm EST.

New Phone Requests and/or Transfer of Phones

To maintain proper asset custody, any cellular repairs, transfers, or returns must be conducted directly between the Telecommunications Specialist and the designated phone holder.

District-Issued Cellular service activations (AT&T) that cannot be initiated prior to 1:00 pm EST will commence on the morning of the following business day.

New district-issued cellular phones will include one protective case and one power charger at the time of initial purchase. The district will no longer provide car chargers. Any additional chargers and protective hardware (cases, screen protectors, etc.) must be provided by the respective department or school.

Before transferring and/or leaving the district, staff that have been issued a district-issued cellular phone **must** submit a One to One Plus ticket and arrange a time to meet with the district's Telecommunications Specialist to wipe and return the phone. This **must** be completed before the employee leaves the position and/or the district.

RICHLAND ONE

Site Issued Cellular Phones

May 3, 2024

Each school and district site has been provided with a cellular phone that is to be used when the VOIP (voice over internet protocol) phone is not in service. The cellular phone should be turned on, and the 3CX app used. When a caller calls the school and/or district's main line the cell phone will ring.

When the school and/or district site needs to call out, they will use the 3CX app to make the calls. Users are to use the 3CX app only to make calls with the cell phone and need to ensure that the phone is connected to the new R1_StaffLink Wi-Fi network. The principal and/or site coordinator that has a district-issued cell phone will need to use their credentials to log onto this network before handing over the cell phone to the user. Principals need to follow the directions outlined on the Network Access for District-Issued iPhones document for connecting to this network.

Principals and site coordinators are to keep the phone in a location that is accessible to the designated staff member that is responsible for answering the school and/or site's main phone line.

RICHLAND ONE

Positions Authorized for Cellular Phones

Updated: May 3, 2023

Assignment of District-Issued Cellular Phones

District-Issued Cellular phones will be assigned to employees in positions listed below.

The Superintendent's Executive Team must approve requests for district-issued cellular phones for any position not on the list.

Staff are to use the updated Cell Phone Request Fillable Form located on the Information Technology Department's Forms webpage. Staff are reminded to use the most updated form and to complete the form electronically, **not print** out and then write on the form.

Board of Commissioners

Internal Auditor	Board of Commissioners
Secretary to the Board	

Superintendent

Chief of Staff	Executive Directors of Schools
General Counsel	Principals
Executive Director AARE	Administrative Assistant to Superintendent
Executive Director of Communications	

Chief of Staff

Director Strategic Partnerships/Extended Day Programs	Coordinator McKinney-Vento
Director Student Support Services	Coordinator Homebound Services
Director Adult Education	Coordinator Volunteers
Lead Coordinator Student Support Services	Social Workers
Coordinator Social Work Services	
Coordinator School Counseling Services	

Chief Finance Officer

Director Accounting
Director Payroll and Accounts Payable
Director Student Nutrition Services
Director Procurement and Warehouse Services

Chief Human Resources Officer

Director Certified Employment Services
Director Classified Employment Services
Coordinator Employee Relations

Director of Budget Services

Supervisor Motor Pool
Supervisor Transportation

Chief of Teaching and learning

Executive Director Elementary Education	Coordinator AAP
Executive Director Secondary Education	Coordinator Montessori
Director Elementary Education	Coordinator Pre-K and School Readiness
Director Early Childhood Education	Coordinator Special Services
Director Special Services	Coordinator Instructional Services Certified
Director Instructional Services	Coordinator Instructional Services Classified
Director Secondary Education	Coordinator Health and PE
Director Federal and State Programs	Coordinator Visual and Performing Arts
Director Learning Environments/Instructional Resources	Coordinator ESOL/World Languages
Director of CATE	Coordinator AVID
	Coordinator Learning Environments and Instructional Resources
	Coordinator Parent and Family Engagement
	Coordinator Psychological Services
	Coordinator Specialized Instruction
	Coordinator PreK – 12 Literacy
	Coordinator Virtual School Program
	Coordinator CATE
	Parent and Family Engagement Specialists

Chief Operations Officer and Budget

Executive Director Information Technology	Maintenance Building Custodial Coordinator
Director Student Transportation	Maintenance Carpenter
Director Building Services	Maintenance Carpenter Crew Leader
Director Facilities	Maintenance Electrician
Director Security and Emergency Services	Maintenance Mason
Director Athletics	Maintenance Master Electrician
Coordinator Technology Support	Maintenance Electrician Apprentice
Coordinator Technology Operations	Maintenance Equipment Operator III
Coordinator Application Support	Maintenance Painter
Supervisor Transportation	Maintenance Paint Crew Leader
Supervisor Motor Pool	Maintenance Plumber
Manager Security Services	Maintenance Plumber Apprentice
Assistant Transportation	Maintenance Plumber Crew Leader
Transportation Officer	Maintenance HVAC Crew Leader
Activity Bus Drivers	Maintenance Glazier
Field Technicians (IT)	Maintenance HVAC Mechanic
Field Technicians (Theater Services)	Maintenance Landscaping Crew Leader
Coordinator Security and Emergency Services	Maintenance Landscaping Specialist
Application Support Staff (IT)	Maintenance Environmental Safety
	Maintenance Mason
	Maintenance Manager of Custodial Operations
	Maintenance Electrician Trade Worker
	Facilities Construction Architect
	Facilities Construction Manager
	Facilities Energy Architect
	Facilities Mechanical Engineer

RICHLAND ONE

Computer Investigation Request (Employee)

Updated: November 4, 2021

If an employee is suspected of violating the district's Acceptable Use Policy, Employee Handbook, or state and federal statutes, a request for an investigation of the employee's devices or accounts may come to Information Technology (IT) from Human Resources and/or Legal Services.

Reporting

a. The requesting party reports the issue to the appropriate source listed above.
b. If the incident appears criminal in nature (nudity, sexual, threats, weapons, pornography, etc.), the Principal/Department Head needs to report the incident to Human Resources. If not criminal in nature, skip to step c.
c. The above-approved source (listed in item a) contacts IT Department by email at ITSecurityInvestigations@richlandone.org to make the request.

Delivery/Pickup

a. Human Resources arranges with the Principal/Department Head and Director of Security to arrange for pickup of the device if the content is possibly criminal in nature. A district asset transfer form should be completed before transfer. The device should be checked in from the teacher in Destiny and checked out to the person taking possession of the device.
b. Principal/Department Head and IT Security Manager arrange for pickup of the device.

Investigation and Reporting

a. IT performs forensic investigation of the device only if necessary.
    - If allegations identify that criminal activity such as nudity, sexual threats, weapons, pornography, etc., no forensic investigation should occur. Human Resources and the Director of Security Services immediately arrange for the device to be delivered to law enforcement.
    - If no such allegations were made and anything is found that violates state or federal law, all investigation is immediately stopped. Immediately report to Human Resources, who will contact the District Security Director to notify law enforcement.
b. Upon completion of the investigation, District IT Security Manager submits the report to the Executive Director of IT for review and signature.
c. Once signed, the report is distributed to Human Resources and the Superintendent.
d. Once all investigation has been completed and the issue resolved, the device will be cleaned and returned to the school/department. Transfer forms are always required. On receipt, the school will check the device back into stock into Destiny.

*At no time should pictures, video, or content that includes nudity, sexual acts, or explicit behavior be emailed or shared in any other manner. Saving personal pictures or video content is prohibited and can lead to consequences such as arrest and/or disciplinary action. Any employee assigned to investigate information regarding this process shall maintain its confidentiality and should not discuss this with anyone other than the superintendent without appropriate permission from Human Resources. *

RICHLAND ONE

Computer Investigation Request (Student)

Updated: January 25, 2021

Discovery

A student is suspected of violating the district's Acceptable Use Policy or state and/or federal statutes.

Reporting

a. Discovering party reports the issue to the school principal.
b. If the incident appears criminal in nature (nudity, sexual, threats, weapons, pornography, etc.) principal needs to report the incident to School Resource Officer. The incident should also be reported to the Director/Manager of Security and IT Security Manager. If not criminal in nature, skip to step c.
c. School principal contacts Information Technology (IT) Department by emailing ITSecurity@richlandone.org to request an investigation.

Delivery/Pickup

a. Principal and District Security Director/Manager arrange for pickup of the device if the content is possibly criminal in nature. A district asset transfer form should be completed before transfer. The device should be checked in from the student in Destiny and checked out to the person taking possession of the device.
b. The principal and IT Security Manager arrange for the pickup of the device.

Investigation and Reporting:

a. IT performs forensic investigation of the device.
    - If anything is found that violates state or federal law, all investigation is immediately stopped. District Security Director/Manager will be contacted as liaison for law enforcement.
b. Upon completion of the investigation, District IT Security Manager submits the report to the Executive Director of IT for review and signature.
c. Once signed, the report is distributed to appropriate parties.
d. Once all investigation has been completed and the issue resolved, the device will be cleaned and returned to the school. On receipt, the school will check the device back into stock in Destiny.

*At no time should pictures, video, or content that includes nudity, sexual acts, or explicit behavior be emailed or shared in any other manner. Saving personal pictures or video content is prohibited and can lead to consequences such as arrest and/or disciplinary action. *

Digital Sign Installation and Support

Updated: May 2, 2024

This process is currently under review.

Those wishing to donate digital signs will need to complete the RCSD1 Public Gifts/Donations/Contribution Verification Form prior to donating the sign. Questions should be directed to procurement@richlandone.org or 803-231-7033.

RICHLAND ONE

District-Issued Devices for All Staff

Updated: July 15, 2024

This document outlines information regarding **all** staff and district-issued devices. There are several changes for the 2024-2025 school year that need to be reviewed.

To become more cost effective and to provide all staff with devices that will allow for portability, we are beginning to transition to laptops with docking stations and a 32-inch monitor as desktop computers become "end of life" for all staff. Once end of life desktops are replaced, we will then transition remaining desktops to laptops with docking stations and a 32- inch monitor.

Eventually, each staff member in the district will be issued **one (1)** device, apart from those that are tasked with work that must be completed on a device that is not portable.

There are some areas, however, where desktop computers will continue to be used and will continue to be replaced at the district level. Those areas are listed below.

Schools/departments do have the ability to use their component budgets to purchase additional devices beyond the **one (1)** that is provided at the district level. They will need to submit a One to One Plus ticket, select Quote and in the description provide the device listed on the Approved Hardware website to request a quote. Review the DRAPE process and the DRAPE Addendum for information on purchasing these devices found on the DRAPE webpage.

Labeling/Coding

Laptops moving forward with be clearly marked with colored stickers to reflect the position that they are assigned to. They will also have that same naming in Destiny. This has been designed to eliminate confusion regarding the various types of devices. As additional names are added, this SOP will be updated.

This is a work in progress. Not all older devices may have stickers at this time. New devices ordered will have stickers.

Device Name in Destiny	Explanation	Etched	Sticker
Teacher Laptop Model	Teacher Laptop with Model Number (Old)	Year TD	NA
DP Laptop	District/Purchased	NA	Name in Explanation
SDP Laptop	School/Department Purchased	NA	Name in Explanation
IADP Laptop	Instructional Assistant District Purchased	NA	Name in Explanation
IASP Laptop	Instructional Assistant School Purchased	NA	Name in Explanation
School Nurse DP Laptop	School Nurse District Purchased	NA	Name in Explanation

Assignment and Checking Out of Devices

The laptops are checked out to a person not to their office or position. All laptops, no matter their purchasing department, are to be checked out in Destiny. Any device not checked out will have the "locked out" message display when the user attempts to log in. Once this replacement cycle is complete, should a staff person move locations within a school say from office 101 to office 102, they would take their laptop with them to their new office. However, if a person is moved from one school/department to another, they would then follow the information regarding Transfer/Moving Positions in the IT SOPs.

Approved Areas for Desktops Purchased at the District Level

- Media Center
  - Circulation Desk
    - Destiny Check-in/Check-out Station (if applicable)
  - Cafeteria
    - Manager
  - Health Room
- School Resource Officer Office

Positions Approved for Desktops Purchased at the District Level

These positions are approved to have two (2) devices and one device must be a desktop. The reason being is that the Security Camera software can only be installed on a desktop. Questions regarding this can be directed to the Security and Emergency Services Department.

- Principal *or* Assistant Principal

Principals need to designate which staff member will receive the desktop to have the software installed.

Next Steps for Desktop to Laptop Transition

When submitting a ticket for a non-functioning desktop device, please select Staff Device as the One to One Plus ticket type and indicate the issue you are having in the description. The technician will determine if a replacement is warranted and if so, he/she will change the ticket type to Staff Device Replacement.

Laptop Inventory for School Staff

Only after a school has reviewed their Destiny inventory, obtained a copy of their property accounting inventory, verified that only the approved staff have the appropriate device, obtained the appropriate documents and turned into Property Accounting for lost and/or damaged devices, and Property Accounting has reviewed the information with the School Laptop Manager or Back-Up Laptop Manager not the Library Media Specialist, the School Laptop Manager may follow the process outlined below to obtain additional laptops for the staff outlined in the next section.

1. Open a One to One Plus ticket.
2. Select Staff Device as the ticket type.
3. Upload the following documents as files for your ticket. (If files are too large, you may need to create a OneDrive file and upload all documents in a file and provide the link to your shared folder. There is a video on how to get a link from a document in your OneDrive so the same directions cane be used for a folder.)
    - Copy of your Destiny inventory
    - Copy of your updated property accounting inventory
    - Copies of completed TVLD forms if applicable.
4. In the description of the ticket, indicate the number of laptops that are needed, the names of staff that need a laptop, and their position (from the list below)
5. Include the following people on the ticket as a person to be notified on update (aka collaborator).
    - Candice L. Coppock
    - Michael Byrnes
    - Johnny Brown

The ticket will be reviewed along with the attached documentation, PowerSchool database for schedules, and Munis for employee information. A determination will be made regarding device information and the ticket will be updated.

Staff Approved for District-Purchased Laptops

Priority for teacher devices, which are those labeled in Destiny as Teacher Device Dell (current model number), is to be given to classroom teachers. Other staff listed below are to receive other staff devices within your inventory, but **not** teacher devices or student devices. Devices can be ordered for non-classroom teachers if you do not have any in your inventory (See Laptop Inventory for Staff on this process.)

Please reach out to Johnny Brown for additional clarification.

- Classroom Teachers (Includes CTE, Itinerate, Related Arts, and Special Education Teachers, as well as Library Media Specialists)
- Interventionists
- Speech Pathologists
- Reading Coaches
- CRTs
- School Counselors
- Instructional Assistants **only** if they have a roster in PowerSchool and are teaching a class. Documentation of a roster will have to be provided to have a laptop.

Staff Approved for District-Purchased Surface Laptops/Pros

- Assistant Principal
- Chief
- Coordinator
- Consultant
- Director
- Executive Director
- Principal

Special Services Specific Laptops

The following staff will receive their devices from the Office of Special Services. Should they have a device issued to them by a school, they will need to return their devices to the School Laptop Manager (SLM) immediately and contact Kendall Jackson at kendall.jackson@richlandone.org to arrange a time to pick up their device at the Office of Special Services offices located at Olympia Learning Center. They must turn their devices back into the Office of Special Services before leaving the district. The devices **are not** to be turned into the school at the end of the year.

- Occupational Therapists
- Physical Therapists
- Audiologists
- Board Certified Behavioral Analysts
- Special Education Instructional Coaches
- Special Education Consultants
- Autistic Itinerant Techers
- Special Education Job Coaches
- Special Education Adaptive PE Teachers
- Special Education Itinerant PreK Teachers
- School Psychologists

Instructional Assistants

New for the 2024-2025 school year. Limited funds were provided to purchase devices specifically for the use of Instructional Assistants. Each school will receive two (2) devices labeled as District-Purchased IA Laptops.

It is up to each school to determine how these devices will be used. However, at any given time, the device **must** be checked out through Destiny. They may not be checked out to one person and then have another person logged into them.

Instructional Assistants are only approved to have the devices labeled as District-Purchased IA Laptops checked out through Destiny. They are **not** approved to check out any other device.

Other Classified Staff

At this time, no other classified staff, such as custodians, ISS Supervisors, etc. are approved to have a district-issued laptop checked out. As a reminder, schools/departments may use their component budgets to purchase school/department devices for these purposes.

Elementary Teacher Carts

- Laptops must be checked out to students and placed in the laptop cart, not checked out to the teacher.
- Carts must be checked out to the individual teacher.
  - Schools are responsible for purchasing locks if the original lock has been lost.
    - Carts will be checked periodically throughout the year.
    - Unattended classrooms are to be locked along when laptop carts are in the room.

Accounting

- All devices must have a current checkout date in Destiny.
- The person checking out the device is the only person that should be logging into the device.
  - Should we see a different log in versus checked out name, the device will be locked and the user will have to bring the device back to the school to have it unlocked.
- Staff who have lost and/or had a device stolen, must follow the district's Theft, Vandalism, Lost and Damaged Report (TLVD) Process.
  - Lost and stolen devices must have a Theft, Vandalism, Lost and Damaged Report (TLVD) completed.
  - Stolen devices must have a police report.
  - **Staff are not to receive a new device until this process has been completed.**

On the Horizon

The district will be transitioning **all** technology inventory, to include SmartPanels, TVs, desktops, laptops, Surfaces, etc. into One to On Plus and **all** technology will be assigned/checked out to all staff and/or a room/location. No portable technology will be provided to a staff member without being checked out through this system. This includes technology purchased at the district and school level.

We will be working with Property Accounting and Warehouse staff over the next few months to create processes and procedures for delivering, entering, and checking out technology in this system.

Training will be provided to all staff that are responsible for maintaining their school's technology inventory. This includes School Laptop Managers, Back-up Laptop Managers, and Library Media Specialists, and may include Bookkeepers.

The intent of this new process is to ensure the district has an accurate inventory of all technology and can develop a plan for replacement cycles.

RICHLAND ONE

Transfer/Moving Positions

Updated: April 23, 2024

District devices are assigned to the location and position, not the person.

If you have a district cell phone, please submit a One to One Plus ticket indicating in the description your current position, school/department, cell phone number, your newly assigned position, and newly assigned school/department. Our Telecom Support Technician will communicate with you via the ticket system to pick up the phone to clear it and prepare for the next user. You must remove your Apple ID and any other personal information from the phone before leaving the district.

Once the phone you will be receiving is obtained and cleared, the Telecom Support Technician will arrange a time to deliver that phone to you.

If you have a laptop that is checked out through Destiny, you will turn that device into your school's Laptop Manager so that it can be checked back into the system. If you have any other laptop/Surface, you will leave that device with a designated person at your school along with any chargers/other cables/dongles that were purchased for the incoming person for your position.

DRAPE Process

Updated: April 26, 2022

Introduction

The DRAPE (Digital Resource Acquisition Process for Expedited) process has been developed to facilitate better review and approval of hardware, software, and other digital resources to:

(1) Ensure that investments in digital resources are aligned with the District's academic and operational goals;
(2) Eliminate duplication of software resources;
(3) Control the proliferation of software titles across the District;
(4) Maintain standardization of hardware on the District's networks;
(5) Confirm compatibility of hardware across the District's networks before purchasing;
(6) Enforce compliance with copyright laws;
(7) Ensure legal review and approval of contracts, licenses, and terms and conditions of use; and
(8) Reduce the time required for approval and authorization to purchase.

No software, hardware, or other digital resources may be purchased without approval and authorization through the DRAPE process regardless of funding source.

Instructions and Reminders for Submitting DRAPEs

Updated: May 2, 2024

- Complete the 2024-2025 DRAPE Form for all DRAPE submissions. The new form is attached and can also be accessed from the Information Technology (IT) DRAPE website. 2024-2025 New DRAPE Form.
  - Include all appropriate or required obtain all appropriate or required signatures (supervisors, directors for federal funds, etc.) before sending to the above-referenced link for review.
  - Attach/submit quotes for all digital resources and request that vendors extend the expiration date of the quote to August 30th of year to allow ample time for legal review and processing requisitions entered in ERP (FORMERLY KNOWN AS MUNIS).

  - Attach the Terms and Conditions, Privacy Policy, and any printed copies of any links that in the document as a PDF (i.e. privacy, student use information, etc.): links are not acceptable.

  - All attached documents must be legible. Documents will be returned to the submitter if pages are incomplete, missing, or hard to read.

- All DRAPES must be emailed to draperequests@richlandone.org. In the subject line of the email, add DRAPE, your school or department name and the name of the resource or product you are requesting (i.e., Subject: DRAPE-Bradley-Smart Panel).
    - DO NOT send forms and supporting documents via district mail.

- Any professional learning that also includes a technology component (online modules, website login, etc.) must have a DRAPE approved prior to submitting the requisition in ERP (FORMERLY KNOWN AS MUNIS).

- Submit the DRAPE packet electronically via the email provided above as one PDF document with documents in the following order: DRAPE form, quote, T&C, Privacy information, other links deemed necessary.

- Multiple DRAPEs from a school/department must be sent as separate emails.

- Any requests submitted after the dates identified in the memo sent out each spring by Dr. Fields must receive Dr. Williams' approval before submitting to draperequests@richlandone.org for IT review.
    - Memos are posted on the DRAPE website.

- If assistance is needed in obtaining a quote for software, staff may enter a One to One Plus ticket and select Quote Request as the ticket type. Include in the ticket the name of the vendor/product, point of contact, number of licenses, item number, and any other essential information needed to assist with obtaining a quote.

- All quotes for technology hardware items must be obtained from the district by submitting a One to One Plus ticket and selecting Quote Request as the ticket type. Include in the ticket the name of the vendor/product, point of contact, item number, and any other essential information needed to assist with obtaining a quote.

- Refer to information regarding the DRAPE Addendum located on the DRAPE website for purchasing a maximum of five (5) items from the district's Approved Hardware List.

- Information Technology (IT) will provide an Information Technology Review Form along with the signed DRAPE that will indicate if the DRAPE has been approved or denied along with additional information regarding the status of the DRAPE.

RICHLAND ONE

DRAPE Addendum

Updated: April 18, 2024

A maximum number of **five (5)** items listed on the district's Approved Hardware list is **exempt** from the DRAPE process. The approved list can be found on the Approved Hardware website located in the Information Technology Standard Operating Procedures document located on the IT Standard Operating Procedures webpage.

Once items have been identified for purchase, users will request a quote by submitting a One to One Plus ticket. All quotes must have Johnny Brown's information and/or signature located on the top. When entering a requisition in ERP (Formerly known as Munis)), users will attach a copy of the Approved Hardware document located on the Approved Hardware website in the Information Technology Standard Operating Procedures.

ERP (Formerly known as Munis)

Updated: May 21, 2024

Why do we use ERP (Formerly known as Munis)?

Schools and Departments use ERP (Formerly known as Munis) to submit requisitions and receive purchase orders. The District uses ERP (Formerly known as Munis) for budgeting, financial reporting, payroll, accounting, fixed asset management, employee benefits, and employee job assignments.

- Employee Self Service (Formerly known as Munis Self Service of Self Service)
  - This is used for all employees to view their paychecks, leave, and update their contact information.
  - If you are having issues with Employee Self-Service (Formerly known as Munis Self-Service of Self-Service), contact Kathy Parker at kathleen.parker@richlandone.org or 803-231-7447or Morgan Bullock at 803-231-7446.
  - HR supports Employee Self-Service (Formerly known as Munis Self-Service of Self-Service).
  - **Do not** submit a One to One Plus ticket for this application.

- ERP (Formerly known as Munis)
  - This is used for those that work in budget, procurement, HR, and finance.
  - Contact the specific department you are having issues with regarding their module.
  - Your log in is your district username and password.
    - Access to certain reports require a different password and username. Should you need this password reset, please use the reset Tyler Technologies Munis Cloud Reset Password Portal link.
      - Should this not work, please submit a One to One Plus ticket.

Access to ERP (Formerly known as Munis)

Requests for access to ERP (Formerly known as Munis) for budget, HR purposes, finance, and procurement must be granted by Human Resources, Finance, and Procurement.

New Account Requests Process for School and Departments (other than HR, Finance, Procurement, and the Warehouse)

- **Do not** submit a One to One Plus ticket requesting access or for your access to be changed. This form must be completed.

1. Staff complete the ERP (Formerly known as Munis)) Account Request Form
2. Request gets automatically routed to the following for approval:
   - HR—Kathy Parker
   - Procurement—LaShonda Outing
   - Budget—Bobbi Jean Flowers and Natasha Kelly
3. IT automatically notified to create the account or make account changes.

Who to Call

Issue	Group/Office	Phone Number
General Ledger Inquiry Training and Budget Information	Budget	803-231-7044
Employee Self-Service (Formerly Known as Munis Self-Service of Self-Service)	Human Resources	803-231-7418
Employee Inquiry	Human Resources	803-231-7418
Employee Personnel Transaction Issues for Termination/Resignations	Human Resources	803-231-7418
Employee Inquiry	Human Resources	803-231-7418
Requisitions/Purchasing Approval Training	Procurement	803-231-7033
Online PO Receiving Issues	Procurement	803-231-7033
Warehouse Requisition Training	Warehouse	803-231-7070

RICHLAND ONE

Event Support

Revised: January 16, 2024

Please see the information below for what **is** and **is not** an IT Event Support.

What is IT Event Support

- An event that is being held after work hours, to include weekends, and requires the department/school to pay for an IT technician to be on site as the event does not have a staff member who is confident that they are able to run the needed technology for the event.
- An event that is being held during the school day that requires streaming (audio and/or video) that has been approved by the superintendent.
- Providing a list of specific URLs (website addresses) needed to be whitelisted if able to do so for the event.
- If visitor Wi-Fi is needed after work hours, a technician is required to be onsite to approve the reservations that are made.
    - Any visitor that needs wireless internet, that the district sponsor(s) must adhere to the new Richland One Visitors Internet Protocols and complete the registration (this form is not to be completed by the visitor) form at least two days prior to the event and provide the visitor with the directions outlined on the website. There is no longer an open guest Wi-Fi. Please remove any signage that has that information posted and let anyone know that reserves the space of this protocols. We do not allow visitors access if there is no reservation completed by the sponsoring department/school.

What is not IT Event Support

- Needing assistance with sound for videos and/or a microphone.
    - A request for support from Theatre Services must be made. Visit the Theater Services Request Forms website for more information.
- Providing cables, cords, connectors, "clickers," etc. for presentations
- Needing computers and/or signing on to computers.
    - There are 3 ways district devices should be used for presentations.
        - If the SmartPanel that is being used has a built-in computer, staff should log onto the device using their district login.
            - No generic logins are to be used.
        - Staff are to use their district-issued device to log on and present.
        - If the presenter is a visitor, they may connect their personal device to the SmartPanel.

If IT support is needed for meetings/events, the office/department requesting the support must submit a One to One Plus ticket **at least two (2) weeks** in advance. Support includes, but is not limited to, a technician and/or access to specific URLs (website addresses) for the event. If the meeting requires support for sound (videos and/or microphones), a request for theatre services support must be made.

1. A Help Desk ticket must be created for any event requiring technical support no later than **two (2) weeks** before the event:
    - All tickets must include:
        1. Date and time
        2. Location
        3. Select Work Type, Event Support
        4. Contact person and select parties' phone numbers
        5. Type of Support requested (do not just put "event support")
        6. URL (website address) if the event needs to connect to
    - Without a ticket submitted two weeks before the event, support cannot be provided.
    - All Event Support Group members will be notified when a ticket is created for review.
    - Group members will make notes in the ticket if clarification from the ticket creator is needed.
2. For any event requiring on-site technology use, at least one successful test run must occur in advance.
3. A budget code must be provided for all events occurring outside of regular work hours to cover overtime for necessary employees.
4. A meeting may be required to obtain additional information regarding the event to identify the number and type of IT staff that are needed in order to support the event.
5. All Communications with technicians must go through the Coordinator of Technology Customer Support.

RICHLAND ONE

Hotspots

Revised: August 22, 2023

Richland One has purchased a limited number of hotspots for student use when they do not have access to Internet use at home to complete assignments that require the use of Internet.

1. School staff send the school's name, grade level, and student's name to hotspots@richlandone.org. This email will be monitored by IT staff hourly.

2. Once IT has verified that the student does not already have hotspot currently checked out to them per the IT's spreadsheet that is updated when requests are made, they will notify the person who sent the email when the hotspot(s) are ready to be picked up from SAB.

3. The school staff person will sign for the hotspot when they arrive at SAB.

4. On receipt of the hotspot the school will check it in to the school site and out of Richland One through Destiny.

5. All hotspots will have a District ID tag. The schools must "check" the device out to the student through the Destiny system.

6. All hotspots will be disabled at the end of the school year and must be collected by the schools, just as you do with laptops, etc.

7. Refer to the Student Laptop Management section for information for end of year collection of hotspots.

iPads

Updated: July 17, 2024

Schools/departments wanting to order iPads must obtain a quote by submitting a One to One Plus ticket and selecting "Quote Request" as the ticket type. iPads must be purchased by the district through the district's account. iPads purchased and/or given as prizes and/or as part of curriculum, etc. will not be allowed on the district's network.

All applications that are needed to be used by a school and/or department that require to be purchased and/or installed must have been DRAPE approved.

iPads that can not be updated to the current operating system, must be sent for discard. Staff must mark these correctly in Destiny and complete and process the **Equipment Transfer Form** found on the IT Department's Forms webpage.

Each student must be assigned his/her own iPad as they would their own laptop. This is because the iPad must be registered in our new Mobile Device Management (MDM) system and Apple School Manager. This is also required for the device to be able to connect to the wireless network.

RICHLAND ONE

ID System Information and Supplies

May 9. 2024

The district's ID System's vendor is Morrison Consulting doing business as (DBA) Access 411. All required materials/supplies for these ID machines, **must** be purchased from this vendor. Their district vendor number is 54612. Using materials/supplies from any other vendor will void our lease agreement and the school/department will be responsible for paying for the full price of a replacement machine.

Requirements for the System

Please note the following requirements regarding the new ID System.

1. Schools have the option to work with the vendor to batch print their IDs at the beginning for the school year (as a cost saving measure) or print them individually on-site.
    - Contact Meredith Collier at Meredith.collier@richlandone.org if interested in batch printing. Schools should make this contact no later than **July 15, 2024**.
2. All student IDs must remain in the district approved **horizontal** clear badge holder.
3. Any sticker supplied by the school may only be adhered to the clear badge holder. Stickers are **not** to be put directly on the ID.
4. Holes **are not** to be punched in the ID as the ID contains a chip that will be damaged if hole punched.
5. Schools must schedule a meeting with the Applications Support Team to discuss any software/program that they are looking to purchase that integrates with the ID System. **No** software/program may be submitted via the DRAPE process without the signature of the Application Support Coordinator, Meredith Collier.
    - Previously purchased software/programs will not integrate with this system.

Responsibilities for the System

Each school has an assigned ID System Administrator, Secondary System Administrator, and Supply Point of Contact responsible for the roles listed below.

ID System Administrator: This is the main point of contact for the ID System at each site. At a school, this must be an administrator. It cannot be a library media specialist, CRT, or any other staff person.

Secondary System Administrator: This is the additional staff member that would be trained to use the system. They would need to be trained and would be listed in the system as a system administrator. This could be a library media specialist, CRT, or other designed staff by the principal. This cannot be a classroom teacher.

Supply Point of Contact: This is the person who orders supplies for your system. At a school, this would be the bookkeeper.

Supplies

We have provided a list of required materials/supplies below as well as optional materials/supplies that the vendor offers as well as a vendor that offers the horizontal required clear badge holders.

As a reminder, these materials/supplies are not part of your Library Media inventory and/or requirements and thus the budget for paying for these should **not** come from your Library Media budget. Please use other budget codes besides those that are allocated to your Library Media Center.

Please email supplies@access411.com to request a quote for the require materials. Please be sure to let them know your school and that you are in Richland One when requesting your quote.

Required Materials/Supplies from Access 411

Item Name	Item Number	Cost
HDP5000 Retransfer Film (750 prints)	405	$121.00
HDP5000 Dual-sided Ribbon YMCKK (500 prints)	402	$238.00
RFID One Card Cards: Mifare Classic 1K White RFID Cards (200 cards)	2086	$260.00
RFID Printer Cleaning Kit- HDP Printer	406	$67.00

Optional Materials/Supplies from Access 411

These materials may be purchased by other vendors and are only provided as reference.

Item Name	Item Number	Cost
3/8 Breakaway Lanyards Solid Colors (No Customization) Minimum 500 lanyards	43-A	.74 each
3/8 Breakaway Lanyards Solid Colors Custom Printed Minimum 500 lanyards	452-BUN	$1.73 each
3/4 Breakaway Lanyards Solid Colors Custom Printed Minimum 500 lanyards	515-BUN	$2.10 each

Required Clear Badge Holders

The vendor BadgePass, Inc. (Vendor ID 52814) is the approved vendor for clear badge holders that can be used both horizontally and vertically (for both students and staff). Contact information for BadgePass is 601-499-2131 or orders@badgepass.com for a quote.

Item Name	Item Number	Cost
Clear Vinyl Multi-Directional Badge Holder (Box of 100)	SA-BSH18151600	$40.00

RICHLAND ONE

Kronos

Updated: Macy 21, 2024

What is Kronos

Kronos is the District's time/attendance and payroll management software.

Kronos URL

Paymasters are the only ones that have access to the website to enter information into the system.
https://richlandone.kronos.net/wfc/htmlnavigator/logon

Employee Badge Request

- All new district employees and contractors, with the exception of short-term substitutes, get their badges from Human Resources.

- At this time, employees that need a new badge must come to the Stevenson Administration Building for a replacement ID. The district is in the process of changing this protocol and process.

- Supervisors who have a contractor working in the district that require an ID badge must complete a form.
    - Contact Regina Harper in Human Resources at regina.harper@richlandone.org.

Install New Clocks

Requests for additional clocks must be sent to finance for approval.

Need Kronos Account

Staff who need an account for Kronos must email Alma Neubig at alma.neubig@richlandone.org. IT does not create Kronos accounts.

Can't Log into Kronos

- Paymasters will use your district credentials (username. last name and district password) to access Kronos.

- Staff need to submit a One to One Plus ticket and select Kronos as their ticket type and enter the message they receive for not being able to log in.
    - Please note that if you have recently changed your district password that you are using your new district password to login.

How to use the clock

- Remove your badge from its holder and place it flat against the upper right-hand corner of the clock.
    - Green light means your punch has been accepted at the clock.
    - Red light means there is an error reading the badge.
    - You should try again, or your badge is not recognized.
        - You need to submit a troubleshooting ticket if the badge is still not recognized.

RICHLAND ONE

Lu Interactive Playground Projectors

Updated: September 12, 2024

The following process has been established to make repairs to the Lu Interactive Playground Projectors located in Elementary Schools.

1. Designated staff members at the school will submit a One to One Plus ticket and select Lu Projectors Interactive Gym as their One to One Plus ticket type.
    - In the description, outline the specific need or issue with the projector.

2. Lu One to One Plus tickets are automatically assigned to the LEIR Consultant in the Learning Environment and Instructional Resources (LEIR) Office and the consultant will add the Director of Technology Services as a collaborator to the ticket.
    - The district replaces damaged bulbs; however, they do not replace damaged remotes.
    - A staff member in the LEIR office will obtain a quote for the new remote and upload that quote as a file to the One to One Plus ticket and indicate a note in the One to One Plus ticket letting the submitter know it has been added.
        - The submitter will need to add a note to the One to One Plus ticket once the new remote has been received.
    - Should a new bulb need to be ordered, a staff member in the LEIR office will order a new bulb and put a note in the One to One Plus ticket once the new bulb has arrived.

3. The Director of Technology Services will add the following staff as collaborators to the One to One Plus ticket:
    - Data Cabling Technician
    - Assigned lift certified district technician
    - Network Security Technician Al Minnigan

4. Once all needed materials have been ordered and/or information from the vendor has been received, LEIR Consultant will put a note in the One to One Plus ticket.

5. The Director of Technology Services will email Darius Moody in Building Services to reserve the district lift.
    - The Director of Technology Services will work with Building Services, Steven Truesdale, and the identified lift certified district technician to identify the date for the reservation.

6. The Director of Technology Services will update the One to One Plus ticket with the confirmed lift reservation date.

7. Steven Truesdale will pick up the lift and deliver it to the location and the lift certified district technician along with Al Minnigan will arrive at the school to work on the projector.

8. Once the work has been completed, verified with the submitter that the projector is fully functioning, the lift certified district technician and/or Al Minnigan will update the ticket indicating the work has been completed.

9. Steven Truesdale will pick up the lift from the school and return the lift. Once returned, he will update the One to One Plus ticket.

10. The Director of Technology Services will email Warren Wingard in Building Services indicating the lift has been returned and put a note in the One to One Plus ticket that the tasks have been completed and mark the ticket as closed.

RICHLAND ONE

Multi-factor Authentication (MFA)

July 15, 2024

- Multi-factor authentication (MFA) is a method of verifying that an end user is who they say they are when logging into systems.

- MFA consists of two basic components:
    1. Something you know (such as a password).
    2. Something you have (such as a code provided by an MFA system).

- **Any** staff member that would like to have access to their Microsoft accounts and other district resources while not on the district network, must have enabled MFA prior to leaving for the school year.

- They must follow the process outlined below.
    1. Open a One to One Plus ticket.
    2. Select MFA as your ticket type.
    3. In the **Description**, provide the following information.
        - Position
        - Location (if you serve in multiple locations, please provide your primary location first and then list all others)
            - Example
                - AC Moore (Primary)
                - Logan
                - Meadowfield
        - Personal Cell Phone Number with Area Code. Google Voice numbers are not acceptable and do not work.
            - Example
                - 18035551236
                    - **Do not** include hyphens, spaces, or parentheses.

Tickets will be closed if they are entered incorrectly and/or missing information.

Network Drives

Coming Soon:

RICHLAND ONE

Network Security Protocols

February 16, 2022

The purpose of the protocols outlined in this section are in adherence to Board Policy IJNDB which ensure that the District will implement measures to prevent internet security breaches, such as hacking, as well as other unlawful activities by students and staff.

Use of Devices

District devices, including cell phones, are not to travel outside of the United States unless approved by the Superintendent or his/her designee for work purposes.

International Logins

The district **will not** approve international logins for students or staff unless approved by the Superintendent or his/her designee for work purposes.

Phishing

Phishing is the fraudulent practice of sending emails purporting to be from reputable companies/individuals to induce individuals to reveal personal information, such as passwords and credit card numbers.

Training Program

Richland One has implemented a training program to educate all users on the dangers of phishing and other related email attacks.

1. Richland One IT will routinely send out phishing emails designed to educate users and simulate actual phishing attacks.
2. These simulated attacks look like actual emails from sources like Microsoft, Google, Apple, etc.
3. These are designed to educate and test the strength of our user's security practices.
4. These simulated attacks help build confidence in users' ability to spot spam, phishing, and the like to prevent actual attacks.
5. Once an attack email is received, IT can track if the email is opened, if anything is clicked, and if credentials are entered.
6. If links are clicked, or credentials entered, the user has failed the test.
7. The user(s) will then be placed into mandatory training provided by our security vendor.
8. Users who have failed the test must complete the training.
9. Users who repeatedly fail the test will have actions set up for their accounts as outlined below.

Training Program Actions and Remediation

1. Initial failure
    - Mandatory training is complete with a short quiz.
2. Failing twice
    - Mandatory training, enrollment into weekly training for three weeks. One training video a week with a short quiz at the end of the training.
3. Third failure
    - Mandatory training, enrollment into weekly testing and training for five weeks, and multi-factor authentication enabled for the user's login.

Actual Phishing Attack Actions

In the event of an actual phishing attack, users who enter information and have their credentials compromised will take the following actions.

- First Event
    - The user is entered into mandatory training with weekly simulated emails for three weeks.
- Second Event
    - User is enrolled in training for five weeks, multi-factor authentication enabled for the user's account.
- Third Event
    - The user account is terminated.

Spam Emails

- If you receive an email that you are not sure if it is a phishing email.
    - **Do not**
        - Open it
        - Reply to it
    - Forward the email as an attachment to spam@richalndone.org

RICHLAND ONE

New Principal and/or Transfer Principal Account Information

June 19, 2024

New principals to Richland One and/or those principals that are transferring to a new school are required to complete the New Principal and/or Transfer Principal Account Information Form located on the Information Technology Department's Forms webpage. The form must be downloaded from the website and completed electronically as there are drop down menus that will not be available if printed. Complete forms are to be emailed to Dr. Candice L. Coppock at candice.coppock@richlandone.org.

A One to One Plus ticket will be submitted for the accounts that Information Technology Department is responsible for creating and then the form will be routed to the other departments. Principals will be copied on the email when the form is sent, and that department will respond to you with information on how to access those accounts.

The form provides information on the various accounts that principals will need access to along with the departments responsible for those various accounts.

RICHLAND ONE

Password Policy (Employees)

Updated: July 9, 2024

Passwords are an essential aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may compromise Richland County School District One's (RCSD1) entire network.

Password Requirements

- All District passwords must be changed at least once every **90** days.
    - We recommend changing your passwords before leaving for the summer for those staff that are not 240-day employees.
    - Use the Password Reset Directions on how to reset your password before it expires.
- **Staff must be on the district network to reset their password. IT staff will not reset staff passwords over the phone.**
- Similar passwords should not be used.
- Adding a number to current passwords is prohibited (e.g., Password01, Password02, Password03…).
- **Do not** write down passwords.
- **Do not** send passwords via email.
- All user-level passwords must conform to the following guidelines:
    - Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters.
    - Passwords must be at least 16 characters in length.
    - Passwords must contain characters from at least three of the following four categories:
        - Uppercase alphabet characters (A–Z)
        - Lowercase alphabet characters (a–z)
        - Numbers (0–9)
        - Special characters or symbols (for example, $#,%)

RICHLAND ONE

Password Policy (Students)

Updated: May 2, 2024

Passwords are an essential aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may compromise Richland County School District One's (RCSD1) entire network. As such, all RCSD1 students are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

STUDENT USERNAME AND PASSWORDS ARE NOT TO BE PLACED ON STICKERS ON DEVICES.

Password Requirements

- All student passwords must be changed at least once every 120 days.
- Similar passwords should not be used.
- Adding a number to current passwords is prohibited (e.g., Password01, Password02, Password03…).
- **Do not** write down passwords.
- **Do not** send passwords via email.
- Teachers **are not** allowed to log in for students.
- Admin and teachers **are not allowed to** set "default passwords" for students or share passwords over insecure means.
- All student passwords must conform to the following guidelines:
    - Passwords cannot contain the user's account name or parts of the user's full name that exceedtwo consecutive characters.
    - Passwords must be at least 12 characters in length.
    - Passwords must contain characters from at least three of the following four categories:
        - Uppercase alphabet characters (A–Z)
        - Lowercase alphabet characters (a–z)
        - Numbers (0–9)
        - Special characters or symbols (for example, $#,%)

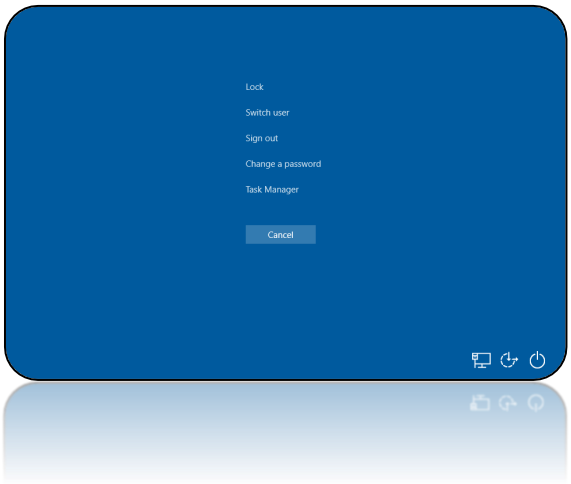
RICHLAND ONE

Password Reset Directions

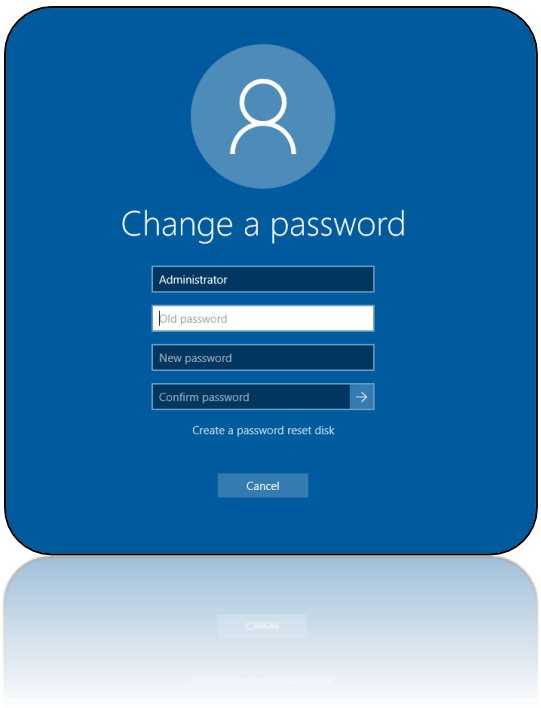
July 9, 2024

Follow these directions to change your password.

1. Press the Ctrl (Control Key), Alt (Alt Key), and Del (Delete Key) at the same time.



2. Click on Change a password (screen will look somewhat like this)



3. Once you enter your information you will click on the small arrow next to Confirm Password and/or pressing the Enter Key

RICHLAND ONE

Parent Use of Devices at District Sites

February 22, 2023

1. **Selection of Equipment to be Purchased**
    a) Determination of need for specific technology is made by the department/school needing the technology.
    b) Determination of specific technology to be purchased is made by the department/school needing the technology.

2. **Purchase Process**
    a) Obtain quotes for devices.
        - Submit a One to One Plus ticket, selecting Quote requests as your ticket type.
        - In the description, be specific in what you are requesting. Do not just put "need a laptop,"
    b) DRAPE approval process must be followed.
        - See the DRAPE Addendum listed on the DRAPE website for or items exempt.
    c) Procurement process if followed.

3. **Arrival of Equipment**
    a) Devices/equipment must be tagged and logged into inventory – Property Accounting
    b) Devices to be setup for use – Information Technology
        1. **Parent account** will be requested to be created- Principal of the School/Site
            - Principal will send an email to NetOps@richlandone.org making the request
            - Principal will include in the email his/her designee that will be contacted regarding the account
        2. Parent account for parent use **only** will be created – Information Technology
        3. Parent account will be locked down for use only on the devices specifically purchased for this reason.

    *Note: This is not referred to as a "Generic Account" as the district does not have generic accounts. These are to be referred to as **Parent Accounts**.*

4. **Post Arrival**
    a) Devices/equipment will be delivered by property accounting to the intended destinations.
    b) Parent account/password will be provided to the designated school/site staff.
        - This account/password is not to be given out to anyone or sent through email or other non-encrypted means.
        - This account/password will only have access to the resource(s) specifically requested.

Printer Guidelines
School Administrators
Updated: May 2, 2024

School Administrators				
Title	**Printer Type**	**Brand**	**Model**	**Specifications**
Principals	Multi-Function Printer	HP	CLJ Pro M4301fdn	33PPM, Color
Assistant Principals	Multi-Function Printer	HP	CLJ Pro M4301fdn	33PPM, Color
Guidance Counselors	Print Only	HP	LJ Pro M4001dn	42PPM, Black and White
- Option 2	Print Only	HP	CLJ Pro M4201dw	28PPM, Color
Bookkeepers	All-in-One	HP	HP OJ Pro 9020 AIO	39PPM, Color
- Option 2	Print Only	HP	LJ Pro M4001dn	42PPM, Black and White
Database Specialist	Print Only	HP	LJ Enterprise M611dn	65PPM, Black and White
Secretary	All-in-One	HP	HP OJ Pro 9020 AIO	39PPM, Color
Administrative Assistant	All-in-One	HP	HP OJ Pro 9020 AIO	39PPM, Color
Media Center	Print Only	HP	LJ Enterprise M611dn	65PPM, Black and White
- Option 2	Print Only	HP	CLJ Enterprise 6700dn	50PPM, Color
Building Custodial Coordinator	All-in-One	HP	HP OJ Pro 9020 AIO	39PPM, Color
Nurse	All-in-One	HP	HP OJ Pro 9020 AIO	39PPM, Color
CRT	Print Only	HP	LJ Pro M4001dn	42PPM, Black and White
- Option 2	Print Only	HP	CLJ Pro M4201dw	28PPM, Color
Cafeteria	Print Only	HP	LJ Pro M4001dn	42PPM, Black and White
SRO Office	Print Only	HP	LJ Pro M4001dn	42PPM, Black and White

- Departments and schools **must purchase their own printers from their component budgets. IT DOES NOT PROVIDE DEPARTMENT/SCHOOL PRINTERS.**
- Zone copiers/printers are available for teachers in every school in the closest proximity to accommodate their printing needs.
- If a teacher wishes to use their annual stipend to purchase their own classroom printer, they must get approval from their immediate supervisor.
    - The printer must be an IT approved model (see the list above).
    - IT does not support these classroom printers.
- Information regarding approved printers can be found on the Approved Hardware list located on the Approved Hardware website. Quotes for one of these printers is to be obtained by submitting a One to One Plus ticket, selecting Quote Requests as the ticket type, and indicating which model number from the Approved Hardware list in the description.
- Staff are asked to reference the DRAPE Addendum located on the DRAPE website regarding items on the Approved Hardware list.

RICHLAND ONE

Quotes

March 23, 2022

To request a quote, staff need to submit a One to One Plus ticket. When opening a ticket, select **ticket type** "Quote Request" and provide details in the description regarding the type of quote that is needed. The quote will be attached to the ticket in the "Files" section.

If any of the requests are for software purchases, IT will provide the quote, however, it is up to the requestor to obtain copies of the terms and conditions, privacy policy, and end-user agreement from the vendor. This information may often be found on the company's website for public access.

Please watch the video for How to Create a One to One Plus Ticket if you need assistance.

RICHLAND ONE

Requesting Email Access and Special Accounts

Updated: May 2, 2024

1. **Requesting access to a former employee's email account**
   Emails and files of former employees are only kept for 45 days following their departure from the district.

   Principal or Department Head send an email to NetOps@richlandone.org for the request.

2. **Requesting Richland One accounts for non-district employees**
   Department Head/Principal must complete the Requesting Richland One Account Microsoft Form. We will not accept forms from anyone submitting on behalf of this person.

   Any entity that does business with Richland One that provides long-term support to the district by way of supporting student instruction and/or working with departments to support students and/or the district such as those listed below may require a Richland One email address to use their agency and/or personal devices.

   The type of account created for each person, depends upon the information provided in the form.

   Approved Groups for Richland One Accounts

   - Teacher Interns (These are submitted through HR. Schools are not to submit teacher intern information.)
   - External Partners with Signed Memorandums of Agreements/Understandings

   Devices/Resources

   - These entities must provide their own devices as they are not approved to be issued a Richland One device as their logins are not created to log onto a district device, however, they are able to access Richland One resources through the web using their Richland One email.
   - They will follow the directions provided on our Richland One Wireless Internet Protocols webpage (https://www.richlandone.org/Page/15036) and connect using the R1_StaffLink wi-fi and are considered "extended quests" when referring to the directions on that website.

   These accounts are only good for one school year. If the user is to return for the following year, a new form will need to be created each year.

3. **Requesting outside email access to/from student email accounts**
   At times there is a need for outside entities to email students, such as those students who are enrolled in courses with Midlands Technical College, students applying to colleges, etc. Should the need arise for those students to receive emails from those outside entities, staff need to follow the steps listed below. All requested entities will be removed from access at the end of the school year. This process will have to be completed each year.

    1. Open an Open to One Plus ticket, select Approval to Email Students as their ticket.
    2. In the files section, upload an Excel file that includes the list of students that need to have this approval.
    3. In the description, include the email address that needs to be approved to send emails to these students.
    4. The address will be vetted as a legitimate educational entity and valid email domain and the ticket will be routed to the next step in the approval process.

4. **Requests for special/shared email accounts/mailboxes**
    1. Requests for special email accounts or shared mailboxes should be submitted through the Information Technology (IT) help desk system, with the ticket type listed as "Email."
    2. The ticket, upon submission, will be assigned to the Network Operations group.
    3. Upon completion, the Network Operations group will contact the requestor to test the account/mailbox to verify successful functionality.

Note: Access to other active users' email accounts is not allowed.

RICHLAND ONE

Saturday SAT Testing Technology School Process

March 1, 2024

The process is to be followed if a high school is going to offer to be a site for Saturday SAT testing. A Richland One technician is **required** to be on-site to approve visitor access to our R1_Visitors Wi-Fi Network. The school is required to arrange payment for the salary of this technician.

Prior to Testing

1. The school must submit a One to One Plus ticket two-three months in advance asking if there is availability for the "event" to be covered.
    - The ticket **must** include in the description.
        - Date
        - Time
        - Hours
        - Budget Code
        - All websites that may need to be unblocked form College Board
    - Incomplete tickets **will not** be processed.

2. If the "event" can be covered, a note will be put in the ticket that the school can proceed with scheduling the testing with College Board and the ticket will be assigned to the technician.

3. The school will need to print copies of the Visitor Access to the Internet directions (school should always check the website for the most updated document (Information Technology / Richland One Visitor Wireless Internet Protocols) to have available to provide to non-Richland One students testing.

4. The following information will need to be displayed clearly via posters, flyers, etc.: Richland One technicians **cannot** provide support (or touch) of any kind other than connecting non-Richland One students' and/or staff's devices to the network by providing printed copies of directions and/or approving the request as it comes in. They **cannot** assist with settings on the student's computer, nor can they assist with installing and/or troubleshooting the Bluebook software.

5. Should the school allow non-Richland One students to test at their site, they **must** inform them that they must download Chrome prior to arriving at the testing site. The test only works on **Chrome.**

Day of Testing

1. The school will set up IT Help Desk area and direct non-Richland One students to after checking in with the proctor.

2. The students will need to have to either have something printed with their name and email address on it or they will have to verbally provide this information to the technician to be recorded on our visitor spreadsheet.

3. The technician will hand them a copy of the directions and record their name and email address on our visitor spreadsheet. Once the student completes the steps on the directions provided to them they will be connected to our wireless network.

RICHLAND ONE

Security Camera Software

Updated: May 2, 2024

Approved staff for security software at the school and/or district site are:

- Principal and/or Site, Department, or Program Director
- Assistant Principal
- SRO
- Security Associate

Those that are approved to have the security camera software installed on **laptops** are **only** the Security and Emergency Services managers and Director.

The process for having software installed on any device is listed below.

1. Approved user will email Security and Emergency Services for access.

2. Security and Emergency Services will submit a One to One Plus ticket.
    - Ticket type: Install Security Camera Software
    - Description: List the name(s) of the staff and their school/site approved for the software (indicate position and if they are approved for laptop installation)
    - Related User: This will be the submitter's name by default.
    - Room Number: This is the submitter's room number by default.
    - Who should be notified on update: List the staff that need to have the software installed.
        - They will be a collaborator and can add notes to the tickets if needed.

3. Network Operations will pick up the ticket and work to have the software installed and will close the ticket when completed.

RICHLAND ONE

SMARTBoard Installation Guidelines

Classroom	Pre-K -2nd Grade
Model	Wall-mounted 6000S Series 65” - PC module with Windows 10 Pro, an i5 processor
Board Height	• Install bottom of board 25” AFF. • Align the bottom of adjacent whiteboards at the same height where possible. • A + 2” variance is acceptable as required by classroom conditions. • Use adjustable mount
Board Installation	• The standard location for the board is centered on the primary teaching wall where the existing board is currently installed. • All new boards should be installed in the exact location of the existing board. NO EXCEPTIONS. • The junction box should be installed directly underneath the panel at 12-18” AFF. • The board will be installed over the Whiteboard, on a Flat Wall, or on a Mobile Stand, depending on the condition of the wall.
Cable Installation	• Cables will be run directly from the panel to the junction box and concealed with the raceway. • A 15’ HDMI cable will be connected to the junction box for the teacher to display images from a laptop. • A 16’ USB-A/Male to B/Male cable will be connected to the junction box for the teacher to have touch capabilities.
Software Installation	SMART Notebook Software, SMART Gallery, and SMART Drivers **MUST BE** installed on the teacher's laptop.

Classroom	3rd -5th Grade
Model	Wall-mounted 6000S Series 65” - PC module with Windows 10 Pro, an i5 processor
Board Height	• Install bottom of board 35” AFF. • Align the bottom of adjacent whiteboards at the same height where possible. • A + 2” variance is acceptable as required by classroom conditions. • Use adjustable mount
Board Installation	• The standard location for the board is centered on the primary teaching wall where the existing board is currently installed. • All new boards should be installed in the exact location of the existing board. NO EXCEPTIONS. • The junction box should be installed directly underneath the panel at 12-18” AFF. • The board will be installed over the Whiteboard, on a Flat Wall, or on a Mobile Stand, depending on the condition of the wall.
Cable Installation	• Cables will be run directly from the panel to the junction box and concealed with the raceway. • A 15’ HDMI cable will be connected to the junction box for the teacher to display images from a laptop. • A 16’ USB-A/Male to B/Male cable will be connected to the junction box for the teacher to have touch capabilities.
Software Installation	SMART Notebook Software, SMART Gallery, and SMART Drivers **MUST BE** installed on the teacher's laptop.

Classroom	6th-8th Grade
Model	Wall-mounted 6000S Series 65” - PC module with Windows 11 Pro, an i5 processor
Board Height	• Install bottom of board 40” AFF. • Align the bottom of adjacent whiteboards at the same height where possible. • A + 2” variance is acceptable as required by classroom conditions.
Board Installation	• The standard location for the board is centered on the primary teaching wall where the existing board is currently installed. • All new boards should be installed in the exact location of the existing board. NO EXCEPTIONS. • The junction box should be installed directly underneath the panel at 12-18” AFF. • The board will be installed over the Whiteboard, on a Flat Wall, or on a Mobile Stand, depending on the condition of the wall.
Cable Installation	• Cables will be run directly from the panel to the junction box and concealed with the raceway. • A 15’ HDMI cable will be connected to the junction box for the teacher to display images from a laptop. • A 16’ USB-A/Male to B/Male cable to be connected to the junction box for the teacher to have touch capabilities.
Software Installation	SMART Notebook Software, SMART Gallery, and SMART Drivers **MUST BE** installed on the teacher's laptop.

Classroom	9th-12th Grade
Model	Wall-mounted 6000S Series 65” - PC module with Windows 10 Pro, an i5 processor
Board Height	• Install bottom of board 40” AFF. • Align the bottom of adjacent whiteboards at the same height where possible. • A + 2” variance is acceptable as required by classroom conditions.
Board Installation	• The standard location for the board is centered on the primary teaching wall where the existing board is currently installed. • All new boards should be installed in the exact location of the existing board. NO EXCEPTIONS. • The junction box should be installed directly underneath the panel at 12-18” AFF. • The board will be installed over the Whiteboard, on a Flat Wall, or on a Mobile Stand, depending on the condition of the wall.
Cable Installation	• Cables will be run directly from the panel to the junction box and concealed with the raceway. • A 15’ HDMI cable will be connected to the junction box for the teacher to display images from a laptop. • A 16’ USB-A/Male to B/Male cable will be connected to the junction box for the teacher to have touch capabilities.
Software Installation	SMART Notebook Software, SMART Gallery, and SMART Drivers **MUST BE** installed on the teacher's laptop.

Classroom	Music, Band, Art, Computer Labs, Science Labs, and Vocational Areas
Model	Wall-mounted 6000S Series 65” - PC module with Windows 10 Pro, an i5 processor
Board Height	• Elementary - Install bottom of board 35” AFF. • Middle - Install bottom of board 40” AFF. • High - Install bottom of panel 40” AFF. • Align the bottom of adjacent whiteboards at the same height where possible. • A +/- 2” variance is acceptable as required by classroom conditions. • Exception: Install bottom of board 36” AFF when the board's view is obstructed. *This mounting height exception will be indicated on all paperwork during walk-throughs.*
Board Installation	• The standard location for the board is centered on the primary teaching wall where the existing board is currently installed. • All new boards should be installed in the exact location of the existing board. NO EXCEPTIONS. • The junction box should be installed directly underneath the panel at 12-18” AFF. • The board will be installed over the Whiteboard, on a Flat Wall, or on a Mobile Stand, depending on the condition of the wall.
Cable Installation	• Cables will be run directly from the panel to the junction box and concealed with the raceway. • A 15’ HDMI cable will be connected to the junction box for the teacher to display images from a laptop. • A 16’ USB-A/Male to B/Male cable will be connected to the junction box for the teacher to have touch capabilities.
Software Installation	SMART Notebook Software, SMART Gallery, and SMART Drivers **MUST BE** installed on the teacher's laptop.

Classroom	Cafeteria Area
Model	Depends on the option selected; see applicable standard above.
Board Height	N/A
Board Installation	Depends on the option selected; see applicable standard above.
Cable Installation	N/A
Software Installation	SMART Notebook Software, SMART Gallery, and SMART Drivers **MUST BE** installed on a standalone laptop or desktop that has to be provided by the school.

Classroom	Gymnasium Area
Model	Two options will be considered in this order: 1. Wall-mounted 6000S Series 65” - PC module with Windows 10 Pro, an i5 processor 2. Mobile 6000S Series 65” - PC module with Windows 10 Pro, i5 processor Note: There is no classroom utilized in conjunction with Physical Education. If there is a classroom, follow the standard for 6th-12th grade classrooms. There must be a secure place for storage.
Board Height	N/A
Projector Installation	N/A – In some circumstances, a project may need to be installed.
Board Installation	Wall-mounted or portable rolling stand.
Cable Installation	N/A
Software Installation	SMART Notebook Software, SMART Gallery, and SMART Drivers should be installed on the teacher's laptop.

Classroom	Media Center
Model	Two options will be considered in this order: 1. Wall-mounted 6000S Series 65” - PC module with Windows 10 Pro, an i5 processor 2. Mobile 6000S Series 65” - PC module with Windows 10 Pro, an i5 processor Considerations for selection include viable wall space for mounting and an appropriate storage location for a portable stand.
Board Height	Depends on the option selected; see applicable standard above.
Projector Installation	Depends on the option selected; see applicable standard above.
Board Installation	Depends on the option selected; see applicable standard above.
Cable Installation	Depends on the option selected; see applicable standard above.
Software Installation	SMART Notebook Software, SMART Gallery, and SMART Drivers **MUST BE** installed on a laptop or desktop that has to be provided by the school.

Classroom	Portable (Mobile Trailer)
Model	Wall-mounted 6000S Series 65” - PC module with Windows 10 Pro, an i5 processor
Board Height	Depends on the option selected; see applicable standard above.
Projector Installation	Depends on the option selected; see applicable standard above.
Board Installation	Depends on the option selected; see applicable standard above.
Cable Installation	Depends on the option selected; see applicable standard above.
Software Installation	SMART Notebook Software, SMART Gallery, and SMART Drivers **MUST BE** installed on the teacher's laptop.

Classroom	Known Special Education Programs
Model	Wall-mounted 6000S Series 65” - PC module with Windows 10 Pro, an i5 processor
Board Height	Depends on the required accommodations.
Board Installation	Depends on required accommodations
Cable Installation	Depends on required accommodations
Software Installation	SMART Notebook Software, SMART Gallery, and SMART Drivers **MUST BE** installed on the teacher's laptop.

OTHER NOTES:

- All existing boards in schools should always be reused if they meet the model standard.
- Verify with the principal that there are no boards stored in the media center, storage closets, etc.
- No boards should be installed in any space less than 300 square feet.
- No boards should be installed in classrooms not currently in use without verification/approval from the Principal.
- Old SMARTBoards defined as surplus by IT, will be stored by the school until Movement Services can pick them up for disposal. Transfer forms must be used to record the pickup.

RICHLAND ONE

School Laptop Management

Updated: May 2, 2024

Introduction

This document outlines the requirements/responsibilities of the School Laptop Manager (SLM) at each school as well as the processes for managing the laptops.

Requirements for the School Laptop Manager

The Principal at each school is responsible for ensuring that all laptops are properly assigned, used and accounted for in accordance with this document and will appoint a SLM to manage these tasks, who must be an administrator at the school. This person **cannot** be a teacher or School Librarian. The rationale is the SLM must be available to complete tasks beyond the 190-day contract. Also, the SLM must have administrator authority at the school in order to enforce some of the tasks.

Additionally, the principal will ensure that someone on staff during the summer is able to log into Destiny and scan in returned devices. Principals are to submit a One to One Plus ticket and select Destiny as the ticket type to request this staff person to have access.

Entering Tickets for Damaged Devices

1. A One to One Plus ticket will be created by the SLM, School Librarian, and/or other designee identified by the principal.
    - The Richland One School technician is not to enter tickets for student/staff devices.

2. The broken laptop will be labeled (a printed copy of the ticket will suffice) and secured in the secure laptop room at each site.

3. When the ticket is assigned, the school's assigned IT technician will begin the process of diagnosis, repair, and/or depot service.

4. When the laptop is repaired, the student should be notified by the library media center that the laptop is ready to return to the classroom.

5. The student will return the loaner and pick up their device.

6. The school will report damaged laptops that are non-repairable to Property Accounting using the District Theft, Vandalism, Lost, and Damage Report (TVLD) process.

Student Devices

July 15, 2024

Richland School District One has a different Standard Operating Procedure (SOP) for the distribution of student devices for the 2024-2025 school year.

It is critical that School Laptop Managers, Back-Up Laptop Managers, and Library Media Specialists adhere to the SOP outlined in this document.

Schools will issue their entire available inventory, regardless of year etched on device, to students at the start of the school year for grades 3-12. Students should keep their device from the previous year if possible, however, this may not be accomplished if those devices are not available due to damages, being in repair, and/or being reported as lost.

PreK-2

- Students will continue to use the devices that have been in circulation since 2020-2021.
    - These are not etched.
    - They are labeled as PreK2 Laptop Dell Education_3190_2-in-1 in Destiny's inventory.
    - The model number on these devices is Dell 3190.
- These devices are to be checked out to an individual student and remain locked up in a cart located in the teacher's classrooms.
- Schools are responsible for purchasing locks if the original lock has been lost.
    - Carts will be checked periodically throughout the year.
    - Unattended classrooms are to be locked along when laptop carts are in the room.
- Stickers with student names can be put on each computer, however, these stickers **cannot** include a student's username and password as this is a violation of the district's **Acceptable Use Policy**.
- Devices that are damaged will need to use the school's existing loaner pool.
    - PreK-2 will not be issued new devices at this time.
- Please review the Processes for Requesting Devices should there be a need to replace out of warranty devices or devices that have been reported as lost/stolen.

Grades 3-12

Schools will issue their entire available inventory, regardless of year etched on device, to students at the start of the school year for grades 3-12. Students should keep their device from the previous year if possible, however, this may not be possible if those devices are not available due to damage, being in repair, and/or being reported as lost.

As a reminder, devices in grades 3-5 will follow the same process for check out and storage as listed in the PreK-2 section of this document. Students in grades 3-5 are not approved to take their devices home daily.

Students in grades 6-12 are approved to take their devices home daily.

The district will review the 2023-2024 135th Day Average Daily Membership Report provided by AARE, as well as the end of the 2023-2024 Enrollment by School and Grade on 05-31-2024 Report provided by AARE. The school will be allocated 6% of the new laptops according to the number of enrolled students for the 2023-2024 school year. All existing devices are to be issued first, reserving the new devices for new students, and as needed.

After the ten (10) day report has been released from AARE, schools can then begin to make requests for additional laptops. However, the following criteria must be met before new devices will be provided.

- A school's Destiny inventory must show that no student has more than one device checked out to them or in repair at a time.
    - Please note that students who are marked as having multiple devices in Destiny **will not** receive an additional device as that device is counted in the school's inventory count.
        - The additional device must be returned before a new device will be provided to the school.
    - Schools are to request this inventory from Property Accounting to ensure that the Destiny inventory matches the Property Accounting inventory.
- A TLVD form must be on file with Property Accounting for each lost/stolen device to receive a replacement.
- When it is determined that a device cannot be fixed and the school does not have available inventory on hand, the school technician will make a request in our ticket system, One to One Plus, for the school to receive a replacement device.

Processes for Requesting Out of Warranty Devices

1. The School Laptop Manager, Back-up Laptop Manager, and/or Librarian would first need to submit a Student Laptop One to One Plus ticket as is the normal process for damaged and/or non-working devices.

2. If it is determined by the school technician that the device cannot be repaired because it is out of warranty, they will change the ticket type to Student Laptop Replacement.

3. The person who submitted the original ticket for the repair will then attach an updated copy of their Destiny Laptop Inventory received from Property Accounting as a File to the ticket (see note about files in tickets **).

4. In the note section of the ticket, the submitter of the ticket will need to provide the following information regarding the student who needs the device:
    - Student Name
    - Student ID
    - Grade Level

5. IT will update the ticket once the information has been reviewed.

Processes for Requesting Lost/Stolen Devices

1. The School Laptop Manager, Back-up Laptop Manager, and/or Librarian will submit a One to One Plus ticket and select Student Laptop Replacement as a ticket type.
    - In the description, provide the following information regarding the student needing the device:
        - Student Name
        - Student ID
        - Grade Level
        - What happened to the device (such as home fire, lost, stolen, unfortunate eviction, etc.)?

2. Upload the following document as a file to your ticket (see note about files in tickets **).
        - Upload a copy of the completed TLVD form and another additional documentation if needed.
            - For information about what is required for TLVD, please refer to the information below.
                - ✓ Property Accounting Forms Website
                - ✓ Financial Services Investigation Procedures for Theft and Lost Property
                - ✓ Instructions for Completing a Theft, Vandalism, Lost and Damaged Report (TVLD)
                - ✓ TVLD Report
                - ✓ TVLD No Police Report Addendum
        - An updated copy of your Destiny Laptop Inventory received from Property Accounting.

- If the file is too large to upload, please create a link for the document and add as a note to the ticket.
            - Please view the video
                - ✓ Information Technology / Creating a Link from a Document in Your OneDrive (richlandone.org)
3. IT will update the ticket once information has been reviewed.

Note about files in tickets:

- If a file is too large to upload to your ticket, the file will need to be put in your OneDrive and then create a link to the file.
    - Paste the link as a note to the ticket.
        - Please view the Creating a Link from a Document in Your OneDrive video for assistance if needed. create a link for the document and add as a note to the ticket.

Additional Information

- When submitting a One to One Plus ticket for repairs for a device, select the student assigned to the device as a related user.

- Any laptop that is not assigned to a student is to be always locked in the laptop room.
    - Schools are to report a broken lock on their laptop room to Security and Emergency Services immediately.

- Cases must always remain on the devices.
    - Devices without cases will not be repaired as they are not under warranty.
    - Schools will be responsible for purchasing lost and/or damaged cases.
        - To obtain a quote for cases, schools can submit a One to One Plus ticket and select Quotes as the ticket type.

- Schools are responsible for purchasing any additional charger that is needed.
    - To obtain a quote for cases, schools can submit a One to One Plus ticket and select Quotes as the ticket type.

- If a student transfers from one school to another in the District, the laptop remains at the student's original school; his/her new school will issue a different laptop.

- At the end of the school year, each school laptop manager will confirm that all student laptops have been returned, checked-in, and stored securely by the year of purchase or, have been renewed in Destiny for use in a Summer Program.

EMAILS ARE NOT TO BE SENT TO JOHNNY BROWN AND/OR SCHOOL TECHNICIANS REQUESTING DEVICES. The above processes have been created and will be followed for the 2024-2025 school year.

Summer Maintenance and Re-imaging

1. During the summer, the student laptops will be maintained, updated, and re-imaged by IT technical support staff.

2. Students in IB programs may keep their laptops during the first part of the summer so they can complete their course work and course tests; re-imaging will be done as soon as the laptops are turned in following those courses.

Student Laptops for Summer Programs

1. If the student is not participating in a District-sponsored summer program, the student is required to turn in their currently checked-out device and hotspot (if applicable) no later than **May 30, 2024**.
    - All devices will be checked back into Destiny.

2. If District-sponsored summer programs require student laptops, those laptops may be provided from the following sources:
    - Middle and High School Students and Virtual Students:
        - Students keep their currently checked out device and a hot spot.
            - Devices are to be renewed in Destiny during the end of year laptop collection process.
        - At the end of the program, the SLM at the school will collect the device and hot spot (if applicable) for check-in in Destiny.
        - If the SLM is unavailable, the school must designate someone to collect the devices and hot spots (if applicable) and check them in.
        - Richland One students using student laptops for summer programs must log in with their District laptops and network credentials; no generic logins will be provided for any student (or adult).
        - Non-Richland One students participating in Richland One sponsored summer programs **will not be** provided a District-owned laptop; no generic logins will be provided for any non-Richland One student.

    - Elementary School Students:
        - Students will turn in their currently checked-out device and hot spot (if applicable) and all other students no later than **May 30, 2024.**
        - Students will be checked out a loaner device Dell 3120s marked 2021-2022 etching device and hot spot if needed for use in the official District-sponsored summer programs from the program manager at the site the student is attending the program to be placed in a laptop cart.
            - Elementary students **will not take these devices home.**
        - At the end of the program, the program manager at the site the student is attending the summer program will collect the device and hot spot (if applicable) for check-in in Destiny.
        - Richland One students using student laptops for summer programs must log in with their District laptops and network credentials; no generic logins will be provided for any student (or adult).

- Non-Richland One students participating in Richland One sponsored summer programs **will not be provided** a District-owned laptop; no generic logins will be provided for any non-Richland One student.

3. Summer programs sponsored and/or provided by non-District/third-party providers will NOT have access to any District-owned laptops for their programs.
    - Such providers MUST provide their own technology and must notify the District that they will be providing their own technology at least six weeks BEFORE the summer program begins (so accommodations can be made for Internet access if needed).
    - The district department and/or school that is "sponsoring" the third-party providing the summer program **must** follow the Richland One Visitors Internet Protocols.
        - As a reminder, there is no "guest" wireless and access must be reserved in advanced and **will not be** granted the day of.
    - Such providers' technology will be subject to all the District's filtering and firewall requirements under CIPA, COPPA, and other relevant federal and state K-12 safety and protection requirements as well as all policies, regulations, requirements, procedures, and practices related to the safe and secure operation of the District's networks.
    - No adult or student users will be provided network or application credentials for access to any resource on the District's network.

RICHLAND ONE

Removing Technology: Student Laptops

Updated: May 2, 2024

NOTE: At this time, this process is on hold. SLMs and Library Media Specialists are asked to spend the end of the year performing inventory clean up. This will be updated when the information has been changed. Please refer to the date of this SOP.

Selection of Equipment to be Removed

Summer of 2024

- Elementary and Middle
  - All remaining Dell 3190s (Student Devices)
- High School
  - Dell 3190s purchased in 2019
    - These devices are etched with "2019-2020."
- **NO OTHER DEVICES ARE ELIGIBLE FOR PICKUP BY THE REMOVAL TEAM.**
- **NO STAFF DEVICES ARE TO BE SUBMITTED TO BE PICKED UP.**
- **TITLE I DEVICES ARE NOT INCLUDED IN THIS REMOVAL PROCESS.**

Pre-Removal Process: School Level

1. The School Laptop Manager (SLM) is responsible for ensuring that they along with the Library Media Specialist and another staff member are available and have access to Destiny to perform the required responsibilities of checking out student laptops.
   - Those that need accounts in Destiny need to submit a One to One Plus ticket and select "Destiny" as their ticket type.

2. Locate a secure designated area for devices that will be removed.
   - This area must be in a secure location that the SLM, the Backup School Laptop Manager (BUSLM) and the Library Media Specialist has access to.

3. Prepare devices for removal from Inventory.
   - As devices are identified for disposal, change the status field in Destiny to "Ready for Disposal."
   - Before the vendor visits to remove the devices, run and print two (2) copies of the "Item Status Report" for devices that are "Approved for Disposal."
   - Confirm that only devices listed in the "Item Status Report" as "Approved for Disposal" are set aside for the Vendor to collect.

4. Schools will receive a schedule from the Information Technology Department.
   - Schools must have their team in place the day of pickup.

Day of Removal: School and Vendor

1. Vendor will arrive at the school and ask for the SLM at the front desk.

2. SLM will provide vendor with a copy of the "Item Status Report" and complete the **Equipment Transfer Form** located on our Forms webpage required by Property Accounting with the vendor staff.

3. The vendor will provide daily updates to the IT and Property Accounting staff.

Post Removal: Vendor

1. The vendor should review equipment picked up from schools and verify that the inventory at the storage site matches the "Item Status Report" provided by the schools.

2. The vendor will provide daily updates to the IT and Property Accounting staff.

3. Discard vendor to coordinate with removal vendor to pick up equipment.

4. Discard vendor to certify wiping of hard disks.

5. Discard vendor to remove district ID tags.

6. Discard vendor will provide inventory report devices that were picked up. This inventory report should be listed by the school and delivered to IT and Property Accounting staff.

RICHLAND ONE

Technology Considerations for Partnerships, Programs, and Projects with Colleges, Universities, Business, and Non-Profit Organizations

Updated: May 2, 2024

K-12 districts and schools are required to control access to and filter content from the Internet (CIPA), protect student and family data (FERPA), and protect student identities and privacy (COPPA) in ways that are not required of colleges, universities, businesses, non-profit organizations, and other public and private sector entities. In addition to those federal requirements, state laws have additional requirements for the protection of students, families, employees, data, networks, and other resources that may be used or accessed through digital means. There are significant consequences for districts, schools, and individuals for non-compliance because those requirements are tied to federal and state funding.

The district and school responsibilities for providing such protections extend to hardware, software, access, storage of data, control of data shared with and used by third parties, the control of data after contractual agreements with third parties have ended, and other related areas.

This document describes the considerations that must be addressed by colleges, universities, business partners, software developers, and providers, non-profit organizations, and other entities (collectively, referred to as partners) that wish to provide programs, projects, after-school activities that require the use of the Richland One network, require access to data about students or staff or collect or create data relating to students or staff.

Network

- The district does not create "generic logins" for students, staff members, or partners.
- All software to be used on or through the district's network must be reviewed and tested at least 30 days prior to its anticipated "go-live" date.
- All hardware to be connected (wired or wireless) to the district's network or to be connected to another device that is connected to the district's network must be reviewed and tested at least 30 days before its anticipated "go-live" date.
- The district's network **will not** be modified (either hardware, configuration, or connections) to support third-party software or hardware.
- The district's wireless network supports only 5GHz connections (older 2.4GHz devices will not connect). Devices not belonging to the district may attach only to the R1_Visitors Wi-Fi networks with limited bandwidth.
- Because the district's network, as well as the state's network to which the district's network connects, are purchased through federal E-Rate funding, the district must comply with E-Rate requirements about prohibiting non-educational use of the network, including the prohibition of individual profit-taking through the use of the district's network.

- Please see the Richland One Visitors Internet Protocols webpage for more information regarding visitors using the district's Wi-Fi network.

Security and Safety

- The district licenses hardware and software to provide firewall services, proxy and caching services, content filtering, and other tools and strategies that comply with federal and state requirements to protect students, staff, and data.
- Those hardware and software resources allow the district to certify that it meets those federal and state requirements because those resources are certified at the national level – meaning that those resources meet at least the minimal requirements for providing the required protection.
- Although those resources allow the district to edit or modify the configurations of those protections, doing so puts the district at risk of nullifying the certifications and assurances that accompany those resources – meaning that the district may invalidate the certification by circumventing the original configurations
    - And, in doing so, the district creates liability for itself and others if students or staff can access "harmful" content or can access and/or expose personally identifiable data.
    - The district has a review process in place to determine the impact of requests to use resources that would be blocked otherwise; such resources should be presented to IT staff at least 30 days before a "go-live" date.
- Partners that wish to use technology-based resources on or through the district's network should work with the District's IT staff to ensure those resources can be accessed without violating the district's security and safety protocols.
- The district is unable to "whitelist" websites and resources that will create non-compliance with federal and state requirements; the district is unable to open ports on its firewall that would jeopardize the security of its network; the district is unable to turn off the proxy and caching services.

Data Access, Storage, Creation, Research, and Disposition

- The district and/or school are the sole and exclusive owners of data collected, stored, shared, or created using all third-party applications, programs, and/or other digital resources.
- Access to and use of student and staff data are of considerable concern for the District.
- Access to and use of student and staff data are subject to federal and state requirements.
- Under federal and state requirements, the district must maintain the security of all its data:
    - Data used for teaching, learning, and operations.
    - Data used for research and after the research ends o Data provided to third-parties, including software applications
    - Data in the hands of third parties, including after contractual agreements end.

    - Data created during the process of use, analysis, and/or reporting o Data kept locally or online o Data retention and/or disposition.
    - Other data
- Protection from loss of data
    - Backup protocols
    - Offsite backups
- Data containing personally identifiable information about Richland One students or staff may not be stored on any server or other device outside the physical and political borders of the United States
    - Such data may not be subject to access, confiscation, or use outside the laws of the United States
    - Such data must be stored and maintained physically where only the laws of the United States may be applied to access, use, or confiscation or seizure.
    - Such data may not be controlled by a company or individual that is not subject to the laws of the United States

Data Used by Online and Cloud-based Applications

- The district and/or school are the sole and exclusive owners of data collected, stored, shared, or created through the use of all third-party applications, programs, and/or other digital resources.
- Currently, most educational resources (like most digital resources for home and business use) are accessed and used online.
- Data required for the successful implementation and management of those resources must be uploaded, typically, to the developer/vendor's servers (in the cloud)
- Contractual agreements with developers and vendors of those resources must include stipulations about the data required by those resources:
    - The district and/or school are the sole and exclusive owners of data collected, stored, shared, or created through the use of all third-party applications, programs, and/or other digital resources.
    - Identification, collection, and use of the data elements required for successful implementation.
    - Ownership of the data remains with the district and/or school.
    - Storage of and access to the data while in possession of the developer and/or vendor
    - Use of the data elements by the software application and the developer/vendor o Inappropriate use of the data elements
    - New data created through analysis of and reporting from the data.
    - Destruction of the original data, new data, and analytics at the end of the contractual agreement
    - No data, in any form, whether anonymized or de-identified, may be kept by any third-party developer and/or vendor without express written consent of the district; no wording within the developer/vendor's contract can replace the requirement that expresses written consent is assigned to the developer/vendor only through a specific attachment or addendum to any such contract.

- Data containing personally identifiable information about Richland One students or staff may not be stored on any server or other device outside the physical and/or political borders of the United States
    - Such data must not be subject to access, use, or confiscation or seizure, outside the laws of the United States
    - Such data must be stored and maintained physically where only the laws of the United States may be applied to access, use, or confiscation or seizure.
    - Such data may not be controlled by a company or individual that is not subject to the laws of the United States

Dual-Enrollment Courses with Partner Colleges and Universities

Richland One partners with several colleges and universities to provide dual-enrollment opportunities for its high school students

- District-owned laptops used by Richland One students are always protected by the district's firewall and filtering resources, whether used at school or away from school.
- Students do not have administrative rights to install software on District-owned laptops. Some of the dual-enrollment courses may include online content that is blocked on the Richland One network and, as such, is blocked on the student's District-owned laptop; if the student is using a Richland One laptop, they will not be able to access that content.
    - In such cases, the student must be able to access that content from a personally owned computer;
    - The District will not whitelist online content that is not appropriate under existing laws and/or regulations
- Some instructors of dual-enrollment courses require students to use a specific "lock-down browser" when taking tests and exams.
    - In those cases, the district can assist the student by installing the lock-down browser (unless it fails to meet security and safety requirements) to complete the course requirements.

Rostering Requirements

- For Richland One, specifically, developers/vendors of software applications that require student or staff rostering must provide a turnkey interface that:
    - Defines data elements required for the rostering.
    - Provides the query and extraction tool(s) that creates the rostering file.
    - Transforms the extracted data into whatever format is required for import into and/or use by the software application.
    - Securely transports the data from the district to the developer/vendor's secure database.
    - Imports or makes the data available to the software application.
    - Provides whatever daily/nightly data update process is necessary for full implementation of the software application.
    - Ensures that the software application functions as expected by the district.

- Potential partners should consider the benefits of creating and using SIS plug-ins that can automate the extraction from the student information system.
- Potential partners should also consider the benefits of using third-party data management applications that can access and acquire information from the District's SIS
- Richland One staff should be involved minimally in this process of rostering (minimally refers to confirming the data elements to be used, providing secure access to those data elements, configuring access for the transport of data to the software application)
- The district and/or school are the sole and exclusive owners of data collected, stored, shared, or created using all plug-ins, third-party applications, programs, and/or other digital resources.

RICHLAND ONE

Testing for Students with Locked Accounts

May 21, 2024

The follow process has been established for those students who have had their district accounts locked due to an AUP violation and need to take the STAR assessment, and/or other district required benchmark assessment or state assessment.

1. The student will go to the designated staff member. The principal may determine this is the Librarian, Assistant Principal, Laptop Manager, etc.

2. That staff member will obtain a student loaner device or the student's device.

3. The staff member will call the Help Desk-Customer Care Center (803-231-7436 or 80000) and provide the student's name and let them know that the student has a locked account due to a AUP violation, and they need to take the X test.

4. The technician will provide a password to the staff member.

5. The staff member will log into the device/program and hand the device to the student. *****The password is not to be given to the student to log in.*****

6. The staff member will monitor the student as they complete their testing.

7. The student will log out of all programs, log off and shut down the computer, and return the computer to the staff member.

8. The staff member will call the Help Desk-Customer Care Center and have the student account locked again**.**

RICHLAND ONE

Technology for Non-District Sites

Revised: January 28, 2021

1. **Selection of equipment to be purchased**
    1. Determination of need for a specific technology (Teaching & Learning)
    2. Determination of specific technology to be purchased (Teaching & Learning)

2. **Purchase Process**
    1. Obtain quotes for technology.
        - Verify that quotes are obtained from contracted vendors (Teaching & Learning)
        - Verify that all necessary components are included on the quote or that accompanying quotes are also obtained (Information Technology)
            - Warranty coverage
            - Tracking software
            - Software licensing
                - 1.e., the district's Microsoft contract does not cover devices that are used at non-district sites
    2. DRAPE approval process (Teaching & Learning)
    3. Procurement process (Teaching & Learning)

3. **Arrival of equipment**
    1. Devices/equipment must be tagged and logged into inventory (Property Accounting)
    2. Devices to be set up for use (Information Technology)
        - Appropriate software purchased with devices to be installed.
            - These devices must **NOT** have Richland One's image.

4. **Post-arrival**
    - Devices/equipment will be delivered by property accounting to the intended destinations.