RICHLAND ONE

Technology Standard Operating Procedures/Processes and Information

Updated 12.10.2025

Updates are noted in purple.

RICHLAND ONE

Table of Contents

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 SOP

Updated: November 18, 2025

Purpose

Define the process for requesting the blocking or unblocking of websites within the organization, ensuring requests are properly routed, reviewed, and actioned according to IT and instructional policies.

Scope

This procedure applies to all staff submitting requests to block or unblock websites for instructional or operational purposes. It also covers the review and approval process for instructional programs requiring account creation for student learning.

Roles

Title	Description of the Role	Role (RASCI)
Requestor (Staff)	Submits ticket for website filtering	Responsible
IT Security Team	Reviews and processes website filtering tickets	Accountable
Library Media Consultant (LEIR)	Reviews instructional appropriateness: routes ticket	Support, Consulted
Teaching & Learning (T&L)	Reviews instructional programs requiring student accounts (DRAPE process)	Consulted
Network Security Manager (IT)	Implements website block/unblock per recommendation	Responsible, Accountable
All IT Staff	Informed of process and outcomes	Informed

Definitions

- **Website Filtering Ticket:** A request submitted via One to One Plus for blocking or unblocking a website.
- **DRAPE:** Digital Resource Approval for Programs and Education; required for instructional programs needing student accounts.
- **LEIR:** Learning Environments and Instructional Resources.
- **T&L:** Teaching and Learning department.

Procedures

#	Description of the Step	Person Responsible (R), Accountable (A)	Supporting (S), Consulting (C), Informing (I)
1	Staff submit a ticket via One to One Plus, selecting IT Security and Website Filtering as the ticket type.	Requestor (R)	IT Security Team (I)
2	If the request is to unblock a website for student account creation, staff must submit a DRAPE; such tickets will be closed.	Library Media Consultant (R) or IT Staff (R)	Library Media Consultant (S), IT Security Team (I)
3	Website Filtering tickets are reviewed by the Library Media Consultant in LEIR for instructional review.	Library Media Consultant (R)	T&L (C), IT Security Team (I)
4	Library Media Consultant documents approval/denial in ticket notes and assigns ticket to Network Security Manager in IT.	Library Media Consultant (R)	Network Security Manager (S), IT Security Team (I)
5	Network Security Team blocks/unblocks site per recommendation, notes completion in ticket, and closes the ticket.	Network Security Team (R, A)	Requestor (I), IT Security Team (I)

Safety and Compliance

- Family Educational Rights and Privacy Act (FERPA)
- Children's Online Protection Act (COPPA)
- Children's Internet Protection Act (CIPA)
- South Carolina Code §59-1-490 (G)
- SCDE SAFE K-12: South Carolina's Assurance Framework for Education Cybersecurity
- School Board Policy GBEBD Use of Technology and AR GBEBD-R Use of Technology
- School Board Policy IJKA Technology Resource Selection and Adoption
- School Board Policy IJNDB Use of Technology Resources in Instruction and AR IJNDB-R Use of Technology

Related Documents and References

- One to One Plus Ticket System
- DRAPE Submission Portal
- Microsoft OneDrive Documentation

Record Keeping Requirements

- Work Order System (One to One Plus)
    - All requests to block or unblock websites must be submitted and tracked through the One to One Plus ticket system.
    - The ticket should include the full URL, the reason for the request, and any supporting documentation.
    - Notes and decisions (approval/denial) are documented in the ticket by the Library Media Consultant and Network Security Manager.
    - The outcome and actions taken (site blocked/unblocked) are recorded in the ticket, and the ticket is closed upon completion.

Notes:

- For Google Files/Forms/Folders, copy the **full** URL into the ticket description (do not use shortened URLs or just email info).
- All instructional programs requiring student accounts must be vetted through the DRAPE process before use.

RICHLAND ONE

District-Issued Cellular Phones

Updated: December 10, 2025

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. A One to One Plus ticket is to be submitted immediately if a phone is defective, lost, or stolen. 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 and must be uploaded as a file to the ticket.

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.

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

Repairs for District-Issued Cellular Phone

Any repairs to district-issued cellular phones must begin with the creation of a One to One Plus ticket. Users must select **Telephone Services** from the Dashboard and then **District Issued 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 Technology Support Specialist 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 1:00 pm 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.

New district-issued cellular phones will include one protective case and one power charger at the time of initial purchase. The district does not 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 are required to 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

Computer Investigations SOP

Updated: November 18, 2025

Purpose

Define the process for requesting, conducting, and documenting investigations of employee and student devices/accounts suspected of violating district policies or laws, ensuring compliance and proper record keeping.

Scope

This procedure applies to all requests for investigation of employee and student devices/accounts within the district, including reporting, delivery/pickup, investigation, compliance, and record keeping.

Roles

Title	Description of the Role	Role (RASCI)
Requesting Party (HR, Legal, Principal, Dept Head)	Initiates investigation request, reports incidents	Responsible
IT Security Manager	Conducts forensic investigation, submits reports, coordinates device handling	Accountable, Responsible
Director/Manager of Security	Coordinates with law enforcement, device pickup	Support, Consulted
Executive Director of IT	Reviews and signs investigation reports	Accountable
Superintendent	Receives signed reports, ensures resolution	Informed
School Resource Officer	Receives criminal incident reports (student investigations)	Consulted
Teacher/Student	Device holder, checks device in/out as required	Informed
Destiny Asset Management	System for device check-in/check-out	Support

Definitions

- **Acceptable Use Policy:** District policy governing appropriate use of technology.
- **Forensic Investigation:** Technical analysis of device/account for evidence of policy or law violation.
- **Destiny:** Asset management system for device tracking.
- **Asset Transfer Form:** Required documentation for device handoff.

Procedures

Employee Investigation

#	Description of the Step	Person Responsible (R) / Accountable (A)	Supporting (S), Consulting (C), Informing (I)
1	Requesting party (HR/Legal/Principal/Dept Head) reports suspected violation.	Requesting Party (R)	IT Security Manager (A), Director of Security (S)
2	If incident is criminal (nudity, sexual, threats, weapons, pornography, etc.), Principal/Dept Head reports to HR.	Principal/Dept Head (R)	HR (A), Director of Security (S)
3	Approved source contacts IT by email (ITSecurityInvestigations@richlandone.org) to request investigation.	Requesting Party (R)	IT Security Manager (A)
4	HR arranges with Principal/Dept Head and Director of Security for device pickup (if criminal). Asset transfer form completed. Device checked in/out in Destiny.	HR (R), Principal/Dept Head (S)	Director of Security (C), Teacher (I)
5	Principal/Dept Head and IT Security Manager arrange device pickup (if not criminal).	Principal/Dept Head (R)	IT Security Manager (A)
6	IT performs forensic investigation only if necessary. If criminal activity is alleged, no forensic investigation; device delivered to law enforcement.	IT Security Manager (R)	Director of Security (C), HR (I)
7	If investigation reveals violation of law, stop investigation, report to HR, who contacts District Security Director for law enforcement notification.	IT Security Manager (R)	HR (A), Director of Security (C)
8	Upon completion, IT Security Manager submits report to Executive Director of IT for review/signature.	IT Security Manager (R)	Executive Director of IT (A)
9	Signed report distributed to HR and Superintendent.	Executive Director of IT (A)	HR (I), Superintendent (I)
10	Device cleaned and returned to school/department. Transfer forms required. Device checked in via Destiny.	IT Security Manager (R), Principal/Dept Head (S)	Teacher/Staff (I)

Student Investigation

#	Description of the Step	Person Responsible (R) / Accountable (A)	Supporting (S), Consulting (C), Informing (I)
1	Discovering party reports suspected violation to school principal.	Discovering Party (R)	Principal (A)
2	If incident is criminal, principal reports to School Resource Officer, Director/Manager of Security, and IT Security Manager.	Principal (R)	School Resource Officer (C), Director/Manager of Security (C), IT Security Manager (I)
3	If not criminal, principal contacts IT by email (ITSecurity@richlandone.org) to request investigation.	Principal (R)	IT Security Manager (A)
4	Principal and District Security Director/Manager arrange device pickup (if criminal). Asset transfer form completed. Device checked in/out in Destiny.	Principal (R), District Security Director/Manager (A)	Student (I)
5	Principal and IT Security Manager arrange device pickup (if not criminal).	Principal (R)	IT Security Manager (A)
6	IT performs forensic investigation. If violation of law is found, investigation stopped, District Security Director/Manager contacted for law enforcement.	IT Security Manager (R)	District Security Director/Manager (C)
7	Upon completion, IT Security Manager submits report to Executive Director of IT for review/signature.	IT Security Manager (R)	Executive Director of IT (A)
8	Signed report distributed to appropriate parties.	Executive Director of IT (A)	HR (I), Superintendent (I)
9	Device cleaned and returned to school. Device checked in via Destiny.	IT Security Manager (R), Principal (S)	Student (I)

Safety and Compliance

- All investigations must comply with district Acceptable Use Policy, Employee Handbook, and applicable state and federal statutes.
- No pictures, videos, or content including nudity, sexual acts, or explicit behavior may be emailed or shared in any manner.
- Saving personal pictures or video content is prohibited and may result in disciplinary action or arrest.
- Confidentiality must be maintained; information may not be discussed except with the superintendent and HR as authorized.
- At no time should pictures, videos, or content that include 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.

Record Keeping

- All investigation requests, reports, and device transfers must be documented and retained according to district policy.
- Asset transfer forms and Destiny check-in/out records are required for all device movements.
- Investigation reports must be signed by the Executive Director of IT and distributed to HR and the Superintendent.
- All documentation must be stored securely and confidentially.

RICHLAND ONE

Digital Sign Installation and Support

Updated: December 10, 2025.

Digital signs that are installed outside of the schools are maintained and handled through the Facilities Management Office. Tickets should be submitted via Brightly.

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

Data and Rostering

Updated: December 10, 2025

Data Access and Data Agreements

Only the **Executive Director of Information Technology** can authorize sending data to vendors with a signed agreement or approved DRAPE.

Richland One requests vendors to sign the Richland One Data Privacy Agreement or the National Data Privacy Agreement. Data will not be provided to a vendor without a signed agreement.

Data Ownership and Security

- The district owns all data collected, stored, shared, or created using third-party applications.
- Data must be stored in the U.S. and comply with U.S. laws.
- Vendor contracts must include terms for data ownership, storage, use, and destruction.
- No data retention by third parties without written consent.
- The district must secure all data used for teaching, operations, research, and third-party services—even after contracts end.
- Personally identifiable information (PII) for students or staff **cannot** be stored outside U.S. borders or controlled by entities not subject to U.S. law.
- Backup protocols, including offsite backups, are required.

Online and Cloud Applications

- The district remains the sole owner of all data in third-party applications.
- Data uploads must be secure.
- Vendor agreements must cover:
    - Data ownership and permitted use.
    - Storage and access during vendor possession.
    - Destruction of all data and analytics at contract end.
- No anonymized or de-identified data may be retained without written consent.
- PII must remain within U.S. jurisdiction and under U.S. law.

Rostering Requirements

- Vendors must provide a turnkey solution for rostering:
    - Define required data elements.
    - Provide extraction tools and secure transfer.
    - Ensure daily updates and proper application functionality.
- SIS plug-ins and third-party data management tools are encouraged.
- District staff involvement should be minimal (confirm data elements, provide secure access).
- The district retains ownership of all data used in rostering and related tools.

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 Technology Standard Operating Procedures/Processes and Information document.

Approved Areas for Desktops Purchased at the District Level

- Media Center
  - Circulation Desk
    - Destiny Check-in/Check-out Station (if applicable)
  - Cafeteria
    - 1 Manager per site
  - 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 Technology Support Specialist 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.
    - 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.

**Should you need assistance with how to get a link to files or folders located in your OneDrive, please see the Information Technology Department SharePoint/Internal Website How to Video Library.

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

Social Workers

Social Workers obtain their devices from the Student Support Services Department. For additional information reach out to Toni Kelly Campbell at antionette.kellycam@richlandone.org.

Instructional Assistants

Limited funds are provided to purchase devices specifically for the use of Instructional Assistants annually. These devices needed to be clearly marked as Instructional Assistant Devices once they are received.

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.**

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 Technology Support Specialist 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 Technology Support Specialist 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.

RICHLAND ONE

DRAPE Process

Updated: April 25, 2025

School board policy, IJKA Technology Resource Selection and Adoption, requires all computer-related hardware, software, and electronic resources to be thoroughly reviewed. The DRAPE (Digital Resource Acquisition Process for Expedited) process is crucial for ensuring the security and integrity of our systems. With rising cybersecurity and data privacy concerns, adhering to this policy and processes protects us from potential threats and ensures a safe digital environment for everyone.

The DRAPE process has been created 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.
(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.

RICHLAND ONE

Instructions and Reminders for Submitting DRAPEs

Updated: December 10, 2025

DRAPEs will be submitted via our new District Routing System (DRS) and Electronic Document Management System (EDMS). To access the application, staff will log into the R1 Portal (ClassLink) and click on the Softdocs DRS_EDMS icon. **No emails nor paper copies of forms will be accepted.**

The only staff that are approved to submit DRAPEs through this system are the following:

Administrative Assistants	Coaches/Consultants/Coordinators	Executive Administrative Assistants
Bookkeepers	Curriculum Resource Teachers	Executive Directors
Chiefs	Directors	Principals

Staff are to refer to the DRAPE memo that was sent out dated April 25, 2025 from Dr. Erica Fields in the LEIR department on the specific information and instructions for submitting a DRAPE.

Staff can also refer to the DRAPE website for additional information.

Updated guidance for the 2026-2027 school year will be provided in the spring.

RICHLAND ONE

DRAPE Addendum

Updated: December 10, 2025

A maximum number of **five (5)** items listed on the district's Approved Hardware list is **exempt** from the DRAPE process.

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.

RICHLAND ONE

ERP (Formerly known as Munis)

Updated: November 19, 2025

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 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 Devonte Coulter at devonte.coulter@richlandone.org.
  - 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 requires 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:
   - Human Resource
   - Procurement
   - Budget
3. IT is automatically notified to create the account or make account changes.

Who to Call for Questions Regarding This Resource

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

IT Event Support SOP

Updated: November 19, 2025

Purpose

Define the process for requesting, providing, and clarifying IT Event Support for district events, including criteria for support, ticketing requirements, and roles involved.

Scope

This procedure applies to all district staff and departments requesting IT Event Support for events held during our regular work hours, including requirements for streaming, visitor Wi-Fi (Internet), and technology setup.

Roles

Title	Description of the Role	Role (RASCI)
Richland One Faculty and Staff	Submits ticket, provides event details, budget code if after hours, and required URLs	Responsible
IT Technology Support Specialist	Provides onsite support, approves visitor Wi-Fi, conducts test runs	Support
Coordinator of Technology Customer Support	Coordinates communication between requestor and Technology Support Specialists	Accountable
Superintendent	Approves streaming requests during school day	Consulted
Production and Performance Technology Services	Provides support for sound, microphones, and related equipment	Support, Consulted
Event Support Group Members	Review tickets, request clarification, make notes	Support, Informed
Department/School Sponsor	Completes visitor internet registration, ensures protocol compliance	Responsible, Informed

Definitions

- **IT Event Support:** Technical support provided by IT for district events, including onsite Technology Support Specialist, streaming, and visitor Wi-Fi.
- Visitor Wi-Fi (Internet) Protocols: District guidelines for registering and providing internet access to event visitors.
- **One to One Plus Ticket**: System for submitting requests/issues related to district technology.
- **Event Support Group:** Team responsible for reviewing and coordinating IT event support requests.
- **What is IT Event Support**
    - After-hours/weekend events require onsite IT Technology Support Specialist due to lack of confident staff.

  - School day events requiring superintendent-approved streaming (audio/video).
  - Providing a list of URLs to be whitelisted for the event.
  - Visitor Wi-Fi after hours (requires onsite Technology Support Specialist and completed registration by sponsor).
- **What is NOT IT Event Support**
  - Assistance with sound for videos/microphones (handled by Theatre Services).
  - Providing cables, cords, connectors, clickers, etc.
  - Providing computers or logins for presentations (staff must use district-issued devices or personal devices for SmartPanel).
  - No generic logins allowed.

Procedures

#	**Description of the Step**	**Person Responsible (R) Accountable (A)**	**Supporting (S), Consulting (C), Informing (I)**
1	Determine if event qualifies for IT Event Support (see "What is IT Event Support" and "What is not IT Event Support" above).	Event Requestor (R)	Technology Support Specialist (S), Coordinator of Technology Services (A)
2	Submit a One to One Plus ticket at **least two weeks** in advance for IT Event Support, including all required details (date, time, location, contact, support type, URLs for websites (No Google sites can be unblocked). *All communication regarding event **must** remain in the ticket.*	Event Requestor (R)	Event Support Group (I)
3	For events outside regular hours, provide a budget code to cover overtime for necessary employees.	Event Requestor (R)	Department/School Sponsor(C) Coordinator of Technology Services (C)
4	For events requiring streaming during school day, obtain superintendent approval.	Event Requestor (R)	Technology Support Specialist (S), Superintendent (C)
5	For visitor Wi-Fi (Internet) after hours, ensure Technology Support Specialist is onsite and Visitor Access Network Request for Wi-Fi (Internet) Microsoft Form is completed by sponsor at least **two days prior**.	Department/School Sponsor (R)	Technology Support Specialist (S)
7	Conduct at least one successful test run for onsite technology use before the event.	Technology Support Specialist (R)	Event Requestor (S)

#	Description of the Step	Person Responsible (R) Accountable (A)	Supporting (S), Consulting (C), Informing (I)
8	If additional information is needed, a meeting may be scheduled to clarify support requirements and staffing.	Event Support Group (A)	Event Requestor (C)
9	Production and Performance Technology Services requests for sound/microphone support must be made separately via Production and Performance Technology Services Request Forms website. *Please review carefully the type of form you are completing.*	Event Requestor (R)	Production and Performance Technology Services (S)
10	Staff (event requestor) and/or presenter are responsible for bringing their own device, cables, connectors, clickers, etc. for presentation as IT does not provide devices and/or these items.	Event Requestor (R), Presenter (R)	NA

Related Documents and Resources

- One to One Plus Ticket System
- Production and Performance Technology Services Request Forms website
- Richland One Visitors Internet Protocols
- R1 Visitor Access to the Internet Directions

Record Keeping Requirements

- Work Order System (One to One Plus)
    - All IT Event Support requests must be submitted through the One to One Plus ticket system.
    - The ticket must include all required event details: date, time, location, contact person, type of support requested, budget code (for after-hours events), and any URLs that need to be whitelisted.
    - Tickets must be submitted at least two weeks in advance; late requests cannot be supported.

RICHLAND ONE

File Storage and Naming Best Practices

March 25, 2025

Personal Work Files

Personal work files are to be saved in staff's Microsoft OneDrive as it provides ample storage and supports collaboration both internally and externally and can be accessed both on and off the district network. Files are **not** to be saved on the desktop of the computer, external hard drives, flash drives, or any other cloud storage such as Google Drive, or Dropbox.

District Files

No district files or records should be stored on flash drives or portable hard drives with the following exception:

- Archival files and records that can be removed from the district network and kept for retention requirements.

Files that are drafts being collaborated on, and/or shared with others, should be kept in a staff member's OneDrive and/or placed in a department's SharePoint/Microsoft Team for collaboration.

IMPORTANT: As a reminder, staff should request that the IT department create a SharePoint/Microsoft Team at the district level and add owners to ensure that all documents created in this SharePoint/Microsoft Team remain after the owner(s) have left the district. Any documents shared from a personally created SharePoint/Microsoft Team may or may not be accessible when that staff person leaves the district.

Network Drives

The Network Drives should only contain final copies of specific district documents outlined below. Access to these files is limited to those with access to the district's Virtual Private Network (VPN). Access is only approved for Principals, Directors, Executive Directors, and Chiefs.

Administrative and Policy Documents

Final copies of

- Policies and Procedures: Official school district policies, procedures, and guidelines.
- Staff Handbooks: Manuals for staff outlining roles, responsibilities, and protocols.
- Board Meeting Minutes: Records of school board meetings and decisions.
- Contracts and Agreements: Legal documents related to staff, vendors, and service providers.

Confidential and Sensitive Files
Final copies of

- Student Records: Academic records, transcripts, and special education documentation.
- Personnel Files: Employment records, evaluations, and other HR documents.
- Financial Documents: Budget reports, financial statements, and audit records.
- Medical Records: Health records and emergency contact information for students and staff if not stored in an online database.

IT and Infrastructure Files
Final copies of

- Software Licenses: Records of software licenses and related agreements.
- Network Configuration: Documentation of network settings, configurations, and security protocols.
- Technical Manuals: Guides and manuals for IT hardware and software used within the district.

Backup and Archival Files
Final copies of

- Disaster Recovery Plans: Detailed plans and procedures for data recovery in case of an emergency.
- Backups: Regular backups of critical files and databases to ensure data integrity and availability

Shared Resources for Large-Scale Projects
Final copies of

- District-Wide Initiatives: Files related to district-wide projects, initiatives, and programs that require broad access but centralized management.
- Professional Development: Resources and materials for district-wide professional development sessions and workshops.

Facilities and Operations
Final copies of

- Maintenance Records: Documentation of maintenance schedules, repairs, and facility upgrades.
- Safety Plans: Emergency response plans, safety protocols, and evacuation procedures.
- Transportation Records: Bus routes, schedules, and transportation agreements.

Best Practices for District File and Record Naming

Electronic records management guidelines recommend that institutions use consistent naming conventions for their files.

- Use a consistent naming convention.
  - Name the file something sensible that others will easily understand.
  - Do not use scanned file names or other formats using random characters
  - Use a logical, repeatable format.
  - Ensure that all team members understand and use the system.
  - Ex. *Department_description_date_version*
    - *IT_Erate-FY25-Cabling-project-Draft_2025-05-19_V02*

- Key Naming Elements
  - Consistent abbreviations
  - Consistent date format
    - Ex. YYYY-MM-DD
  - Concise but informative description
  - Use hyphens between words
  - Include draft/final status
  - Number versions systematically

- Things to Avoid:
  - Special characters - !@#$%^&*()
  - Overly long filenames
  - Vague descriptions

RICHLAND ONE

Google Applications and Google Chrome Extensions

Updated: December 10, 2025

Google Applications

Google Docs and Google Drives are not approved for Richland One Use. We are a Microsoft district, and files are to be saved in Microsoft One Drive.

Material that is to be used for students is to be used through an approved resource, which is Microsoft. You will need to save district related material when you are at home, not on district network to your district Microsoft OneDrive account.

Due to inappropriate content, parts of Google are blocked in compliance with the Child Internet Protection Act. As a result, Google Docs and other Google apps are not consistently accessible.

We will continue to periodically block these resources as potential risks are identified to our system.

YouTube which is a Google application is allowed within the Richland One environment using your Richland One log in credentials.

Staff who participate in Google Meets with other districts may do so with their Richland One credentials as well. Staff that experience any issues with this application are asked to submit a One to One Plus ticket and select IT Security from the Dashboard and then Website Filtering as your ticket type. This must be completed at **least 5 days prior** to the event. You are asked to provide the specific URL for the meeting in the description.

Staff who have been provided URLs Google Files, Forms, and Folders by SCDE, SCASA, and other organizations to be reviewed need to see the information outlined in the Blocking and Unblocking Websites section of this Technology Standard Operating Procedures/Processes and Information document.

Google Chrome Extensions

Staff may submit a One to One Plus ticket and select **Application Support** from the Dashboard and then **Chrome Extensions** from the Category 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.

Staff who may need assistance approving videos can view our Information Technology Department SharePoint Internal Website and click on the How to Videos Library.

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: December 10, 2025

Schools/departments wanting to order iPads must obtain a quote by submitting a One to One Plus ticket and selecting **Quotes/Printers/Hardware** from the Dashboard and then **Quote Requests** from the Category options. 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 need to be used by a school and/or department that require purchased and/or installed must have been DRAPE approved.

iPads that cannot 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 and/or staff 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

Updated: March 4, 2025

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.
    - Meredith Collier will post information regarding this option each spring for the upcoming school year in the R1 ID System Microsoft Team.
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 designated 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 Smith's Addressing Machine Service (Vendor ID 55839) is the approved vendor for clear badge holders that can be used both horizontally and vertically (for both students and staff). Contact information Smith's Addressing Machine Service is sales@sams1.com.

Item Name	Item Number	Cost
Clear Vinyl Multi-Directional Badge Holder (Box of 100)	1815-1600	$40.00

RICHLAND ONE

Lu Interactive Playground Projectors

Updated: December 10, 2025

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 Technology Support Specialist
    - Assigned lift certified district Technology Support Specialist
    - Network Security Technology Support Specialist 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 Facilities Management to reserve the district lift.
    - The Director of Technology Services will work with Building Services, Steven Truesdale, and the identified lift certified district Technology Support Specialist 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 Technology Support Specialist 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 Technology Support Specialist and/or Courtney Paige 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)

Updated: December 10, 2025

To enhance our security and protect sensitive information, the district began requiring Multi-Factor Authentication (MFA) for **all** staff effective December 20, 2024. MFA is required to access district resources without being connected to the district network.

It is the responsibility of the employees' supervisor to review this information once they are hired and onboarded.

To enable MFA, the **individual staff person** must submit a One to One Plus ticket, select **MFA** as their ticket type and provide the following information in the description (do not enter the phone number in any other area of the ticket). **Incorrect ticket types or those tickets with missing information will be closed.** Please note that it may take 5-7 business days to process these tickets.

- Personal cell phone number with area code. Google Voice numbers do not work.
    - *Example (type out phone numbers as listed below)*
        - 18031234567
            - **Do not** include hyphens, spaces, or parentheses.

Staff who may need assistance with accessing their account with MFA, they can view the **Accessing your Account with Multi-Factor Authentication Directions** located on the Information Technology Department SharePoint Internal Website. This document is found under the Resources tab and the How To Documents folder on this site. The document will need to be downloaded prior to leaving the worksite as you will not have access to the document off the district network.

Staff that already have MFA enabled **are not** to submit another ticket.

Staff that have MFA enabled but are getting an error message or a locked account message, need to submit a One to One Plus ticket, and provide that information in the description of their ticket so that their account can be unlocked.

If staff change cell phone numbers anytime during the year, they will need to submit a One to One Plus ticket, select MFA as their ticket type, and provide their new phone number.

Staff should note that if they enter the incorrect code too many times, their account will lock, and they will need to submit a One to One Plus ticket, select MFA as their ticket type, and request their MFA account to be unlocked.

Pease note that it may take 5-7 business days to process these tickets.
Tickets will be closed if they are entered incorrectly and/or missing information.

What is Multi-factor Authentication?

- Multi-factor authentication (MFA) is a method of verifying that an end user is who they say they are when logging into systems.
- Multi-factor authentication (MFA) consists of two basic components:
    - Something you know (such as a password).
    - Something you have (such as a code provided by an MFA system).
- This is the same type of system that people may be familiar with when making online purchases.
    - When logging in, some websites will send a code to an email address or text to a cell phone to enter to verify.

Why Multi-factor Authentication?

- One of the biggest issues that we see in the technology world today is fraudulent emails such as phishing attempts.
- Phishing attempts try to get users of our technology systems to click on links that take them to pages which present themselves as legitimate sites in an effort to have them make purchases of items such as gift cards and send them to the bad actor or to obtain their network credentials.
    - A bad actor is a person/entity that is making a phishing attempt.
- With these credentials, the bad actor can then login to systems and use their access to obtain data or funds.
- Multi-factor authentication (MFA) prevents this by requiring a code that the end user has with them in order to access the network. Without this code, even with the users' credentials, the bad actor cannot access systems.

Network Security Protocols

Updated: December 10, 2025

The purpose of the protocols outlined in this section are in adherence to Board Policy IJNDB Use of Technology Resources in Instruction and GBEBD Use of Technology 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. These requests must be emailed to the Executive Director of Information Technology no later than two weeks prior to travel. Users who attempt to access their accounts that have not been approved will result in a locked account. They will have to contact the Customer Care Center/Help Desk at 80000 once they arrive back on district network to have their passwords reset.

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
- Staff should also click on the **Report** feature in Microsoft Outlook in order to report the email to Microsoft.

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: March 6, 2025

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, $#,%)

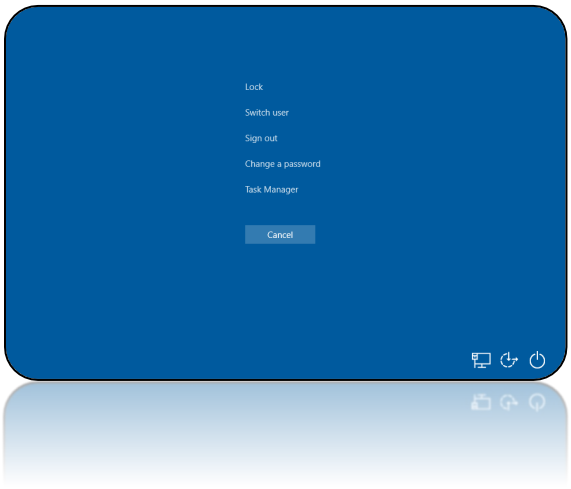
RICHLAND ONE

Password Reset Directions

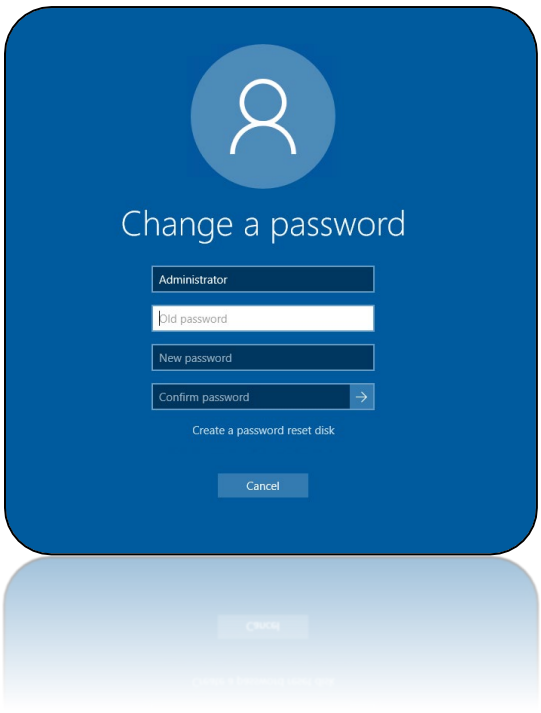
July 9, 2024

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

Updated: December 10, 2025

Please be reminded that staff **are not allowed** to log into any device and allow anyone to use their device. This is referenced in both Administrative Rule AR-IJNDB-R Acceptable Use of Technology and AR-GBEBD-R Acceptable Use.

1. **Selection of Equipment to be Purchased**
   Review the list of approved laptops on the Approved Hardware list. Department/School may reach out to the Technology Asset Manager, Jonathan Vazquez, for suggestions if needed.

2. **Purchase Process**
   a) Obtain quotes for devices.
      - Submit a One to One Plus ticket, select **Quotes/Printers/Hardware** from the Dashboard and then **Quote Requests** from the Category options.
      - In the description, list the specific laptop selected from the Approved Hardware list or the specific one that was provided by the Technology Asset Manager, including the quantity.
        - Do not just put "need a laptop,"

   b) DRAPE approval process must be followed for any item that is not on the Approved Hardware list.
      - 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 accounts 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.

RICHLAND ONE

Printers

October 15, 2024

Please note the following regarding printers.

- Zone copiers/printers are available for teachers in every school in the closest proximity to accommodate their printing needs.

- Departments and schools must purchase their own printers from their component budgets. **IT DOES NOT PROVIDE DEPARTMENT/SCHOOL PRINTERS.**

- If a teacher wishes to use their annual stipend to purchase their own classroom printer, they must get approval from their immediate supervisor. IT does not support these classroom printers.

Admin Area Printers

The district is providing a quote for this printer, however, please note the following. The district will provide limited support for this printer as zone printers are furnished for district use. These printers will be hardware connected to the network but are not approved to be connected to the wireless network.

IT will provide limited assistance once they are installed. School staff should be prepared to conduct their own basic troubleshooting such as removing paper jams, replacing ink, etc. Schools, departments, and staff are purchasing knowing these stipulations.

Individual Computer Printers

The district is providing a quote for this printer, however, please note the following. The district will not provide any support for this printer as zone printers are furnished for district use.

These printers will not be connected to the network, are not to be connected to the wireless network, will receive no assistance from IT if they require a driver to be installed, and will receive no troubleshooting for IT. Schools, departments, and staff are purchasing knowing these stipulations.

Any printer that is purchased using Richland One funds, must be a printer that is on the **Approved Hardware list** and/or listed on the following page.

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

Approved Printers for Areas

Updated: October 15, 2024

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

RICHLAND ONE

Quotes

Updated: March 6, 2025

To request a quote, staff need to submit a One to One Plus ticket. When opening a ticket, select **Quotes/Printers/Hardware** from the Dashboard and **Quote Request** as the ticket type 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

Removing Technology: Any Technology

November 19, 2025

Any device that is no longer functioning and needs to be disposed of can be sent to the warehouse for disposal. The following steps must be taken.

1. Device needs to be marked appropriately in Destiny (if applicable).
2. Complete an Equipment Transfer Form (form is located on the IT Department Forms Website.)
    - The form has 10 lines so if you are disposing of more than 10 items, additional forms will need to be completed.
3. Print a copy of the form and affix on the stack of computers that have been marked for disposal.
4. Contact your Building Coordinator and let them know that you need them to submit a Brightly work order to have the Warehouse pick up the devices for disposal.
5. Email a copy of the completed Equipment Transfer Form to Mike Byrnes at michael.byrnes@richlandone.org.

RICHLAND ONE

Requesting Email Access and Special Accounts

Updated: November 19, 2025

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**

   As part of our ongoing commitment to maintaining a secure and compliant data environment, we are updating the process for requesting accounts for individuals who are not employed by Richland One.

   Requests must include a signed copy of the Richland One Vendor Access Agreement. This agreement can be found on Requesting Richland One Accounts Microsoft Form. It is critical that staff use the most updated version that is posted on this Microsoft Form.

   This requirement is a critical step to ensure that any external access to our systems aligns with district-approved security protocols and legal standards. It reflects our continued efforts to safeguard sensitive information and uphold the integrity of our digital infrastructure.

   Department Head/Principal must provide vendors or contractors with the most up to date copy of the Richland One Vendor Access Agreement to complete and return to you. The signed agreement must be uploaded as a PDF when submitting the Requesting Richland One Accounts Microsoft Form.

   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 submitting 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 **IT Security** from the Dashboard then **Approval to Email Students** from the Category type.
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**
   At times there is a need to request a shared email account be created where several people will need to receive inquiries. For example, a school would like to have an email where parents can send concerns to so they would request and email to be created called "ABC Elementary Parent Concerns." The following process needs to be followed in order to make this request.

   1. Open an Open to One Plus ticket, select **Microsoft Application** from the Dashboard then **Microsoft Outline Email** from the Category type.
   2. In the description, provide detailed information on the name of the email you would like, the purpose and who will need access to this email.
   3. Include those that need access to the email as collaborators to the ticket.
   4. Once the email has been created, notes for how to access the email will be uploaded by IT staff so that everyone has the information and the ticket will be closed.

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 Technology Support Specialist 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 Technology Support Specialist.

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 Technology Support Specialist.

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 Technology Support Specialists **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 Technology Support Specialist to be recorded on our visitor spreadsheet.

3. The Technology Support Specialist 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

SCDE Web Portal

Updated: December 11, 2025

The SCDE Web Portal is the portal that is used for identified district and **some** school designated staff such as principals, school counselors, social workers, etc. that must log in to complete various tasks. This portal is **not** for teachers. Teachers who need to access their teaching certificate, submit renewal credit, etc. are to use the My SC Educator Portal. More information about this portal can be found by accessing the SCDE My SC Educator Portal website. The IT department does not maintain the accounts for this portal as we only handle the SCDE Web Portal accounts.

Staff are instructed to **not** use the "Forgot your password" or "Don't have an account" features located on the SCDE Web Portal landing page.

If you require a **new** SCDE Web Portal account, you need to follow the steps outlined below.

1. Open a One to One Plus ticket.
2. Select **Application Support** from the Dashboard then **SCDE Web Portal** from the Category types.
3. In the description, provide the following information.
    - Your role in the district.
    - The specific full name(s) (no acronyms) of the application you need to be assigned.
    - The specific full role(s) (no acronyms) of the application you need to be assigned.

You need to find out from your supervisor and/or person at the district office or SCDE the specific names of both the application and roles that must be assigned. Your account will not be created until these are provided.

If you need to have a password reset and/or get an error when trying to log in, you need to follow the steps outlined below.

1. Open a One to One Plus ticket.
2. Select **Application Support** from the Dashboard then **SCDE Web Portal** from the Category types.
3. In the description, provide the following information.
    - Indicate that you need your password reset and/or that you are having issues logging in.

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

Updated: December 11, 2025

District purchased SMARTPanels come with the following:

- Built-in Micro-PC (personal computer)
- HDMI Cables for connecting laptop
- Wireless keyboard and mouse
- Pens
- All teachers have access to the SMARTNotebook software which is now called Lumio. It is web-based and can be accessed via the R1Portal (ClassLink). There is no software to download.

Standard Heights

- PreK-2nd Grade
  - Install bottom of board 25" AFF.
- 3rd- 5th Grade
  - Install bottom of board 35" AFF.
- 6th – 12th Grade
  - Install bottom of board 40" AFF.
- Gymnasiums, Media Centers, Other Classrooms
  - Installation will depend upon the room and/or Mobile panels are an option.

General Installation Requirements

- The standard location for the board is centered on the primary teaching wall where the existing board is currently installed.
- All new boards are to be installed in the exact location of the existing board.
- Boards must be installed over the Whiteboard, on a Flat Wall, or on a concrete/cinder block wall.
- Boards are aligned to the bottom of adjacent whiteboards at the same height where possible.
- A + 2" variance is acceptable as required by classroom conditions.

RICHLAND ONE

School Laptop Management

Updated: December 11, 2025

Please note that an updated Laptop SOP is currently being updated and will be updated here as soon as it has been approved. Until such time, we will use these processes/practices.

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 administrative 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 Technology Support Specialist 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 Technology Support Specialist 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.

RICHLAND ONE

Student Devices

Updated: December 11, 2025

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

- 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**.
- 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 devices 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 **3-8 are not approved** to take their devices home daily.

Students in grades 9-12 **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.

Processes for Requesting Devices: Out of Warranty, Contaminated, Stolen, or Lost

1. The School Laptop Manager, Back-up Laptop Manager, and/or Librarian will submit a One to One Plus ticket and select Computers from the main Dashboard and then will select the type of computer that is being request (Student Laptop or Teacher Laptop) as the ticket type.

2. Complete each part of the ticket.
    1. Description of Damage
        - In this section, there must be a description of what happened to the device. This must be completed and needs to be specific.
            - *Example:* Screen shattered, and hinges broken.
                - *If it is out of warranty, simply state, Out of Warranty.*
    2. How did the damage occur?
        - In this section, there must be a reason as to how the damage occurred. Tickets with NA will not be processed.
            - *Example:* Student John Doe was in class and another student walked by and knocked John's laptop off his desk. The screen was shattered, and hinges broken.
                - *If it is out of warranty, simply state, Out of Warranty.*
    3. What date did the incident occur?
    4. Enter the District ID Number (ex. 999…)
        - Please note that you must enter the numbers very slowly and they will populate.
    5. Asset Type
    6. Related User
        - Type in the name of the student/staff member that the device belongs to
    7. Site
    8. Phone number
        - Please also put their 3CX extension (no personal cell phones)
    9. Room Number
    10. Collaborator

Note: Devices that have been identified by School Laptop Managers, Librarians, IT Staff, and/or eBryIT staff as being intentionally damaged will be either returned from eBryIT and/or not sent to eBryIT for repair. If the devices can be repaired in house using parts that we have on-hand the IT Technology Support Specialist will make such repair. However, the students who have intentionally damaged the device should not be given a loaner device to replace the intentionally damaged device to be used continuously. The school should develop a process by which the student checks out the device in the morning, use the device during the day, and then returns the device before leaving.

Devices without information provided will not be evaluated by either the IT Technology Support Specialist until information has been provided. Additional student laptops will not be provided for intentionally damaged devices.

Upload the following document as a file to your ticket if required (see note about files in tickets **).

- 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

- Upload a copy of the completed TLVD form for lost or stolen devices only.
- Upload any other supporting documentation you wish to provide.

3. The School Technology Support Specialist will review the ticket and determine if the ticket is to be moved to a Laptop Replacement Ticket type for review.

4. IT staff 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. Videos can be found in the Information Technology Department Internal SharePoint/Website. 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.

- Laptop 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 chargers that are 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 JONATHAN VAZQUEZ AND/OR SCHOOL TECHNOLOGY SUPPORT SPECIALISTS REQUESTING DEVICES.

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

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 whether 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 Technology Support Specialist 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 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.

RICHLAND ONE

UKG (Formerly UKG)

Updated: December 11, 2025

What is UKG (Formerly known as UKG)

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

Accessing UKG

UKG is to be accessed via the district's R1 Portal (ClassLink). The R1 Portal can be accessed directly from the district's main website. It can be found in the Green Financial Services Folder.

Install New Clocks

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

Need UKG Account

Principals/Supervisors must complete the UKG Access Approval Form for any staff that is a new Paymaster/Approver and/or if changes need to be made to an existing Paymaster/Approvers' account. This includes permanent and temporary access.

https://forms.office.com/r/x31QND54qk

Can't Log into UKG

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

- Staff need to submit a One to One Plus ticket and select UKG 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

YouTube

Updated: December 11, 2025

- 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 YouTube Approval video located in the IT How to Video Library in our Information Technology Department Internal SharePoint Website.

Please note that IT will not unblock YouTube videos through the Website Filtering ticket type in One to One Plus.

RICHLAND ONE

Virtual Private Network (VPN) Global Protect

Updated: December 11, 2025

The use of Richland One's VPN (Global Protect) is only for those staff that need to work within the Human Resource, Procurement, Finance and/or Budget modules in ERP (formerly known as Munis) and/or on rare occasions department's Network Drives Files when not connected to the district's network. These staff must also have Multi-factor Authentication (MFA) enabled.

Staff that are approved for Richland One's VPN are:

- Chiefs
- Executive Directors
- Directors
- Principals
- Staff approved at the Chief level

To ensure district resources are accessed appropriately, district staff who are approved to have access to the VPN (Global Protect) must complete an annual training session each year to maintain their access.

Approved users, Chief, Executive Director, Director, and Principal, will follow the process outlined below to obtain access to VPN.

1. The requestor opens a One to One Plus ticket.
    - Users cannot have someone else submit a ticket on their behalf.
2. Select **Network Connectivity** from the Dashboard, then V**PN Access Request** as the Category.
3. IT staff will provide the required training video with a Microsoft Form that has to be completed.
    - Once the video is viewed and the form is completed, the request for VPN will be approved and the ticket will be moved to a Technology Support Specialist to have the VPN client, Global Protect, installed.

Any staff requesting access that is not considered an approved user will first require Chief approval via the ticket system before the required training video and Microsoft Form will be provided.

Questions can be directed to Dr. Candice L. Coppock at candice.coppock@richlandone.org.

RICHLAND ONE

Visitors, External Partners, and Dual-Enrollment

Updated: December 11, 2025

K-12 districts and schools must comply with federal and state laws to protect student data and privacy, which include CIPA, FERPA, and COPPA. Non-compliance can lead to significant consequences, including loss of funding.

Visitors

Richland School District One network is for educational and instructional purposes only. Programs that are for-profit (day-care providers, companies/organizations running a business on school grounds, etc.) are not eligible to have access to our network. Visitors who come to Richland One for one of the reasons below are eligible to have access to the district's R1 Visitor Wireless Network:

- Professional learning with a department/school.
- Presentation with a department/school.
- Working with students (student teacher, consultant, guest lecturer, etc.)
- Conducting business with a department/school.

Please see the Richland One Visitors Internet Protocols webpage for more information regarding visitors using the district's Wi-Fi network as well as Richland One Visitor Wireless Internet Protocols outlined in this document.

Please note:

- Network modifications for third-party software/hardware are not allowed.
- Only 5GHz wireless connections are supported; visitors use limited bandwidth Wi-Fi.
    - Devices not belonging to the district may be attached only to the R1_Visitors Wi-Fi networks with limited bandwidth.

These visitors do not qualify for a Richland One email account.

Accounts for Non-District Employees

Richland One does not create generic logins for any users. District sponsors that work with organizations that have partnerships with the district that as a part of their memorandum of agreement that require a district login are to refer to the Requesting Email Access and Special Accounts Standard Operating Procedure outlined in this document.

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 are not permitted to download and 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.

RICHLAND ONE

Richland One Visitor Wireless Internet Protocols

Updated: December 11, 2025

The R1_Visitors (School/Site Name) Wi-Fi network is for educational and instructional purposes only. This network has been established for those that are not affiliated with the district and do not have Richland One email accounts. All requests for access to the network **mus**t be made in advance to authenticate the use of the visitors.

Department/School sponsors for visitors, who meet the criteria for using the network as outlined below, **must** complete the Richland One Visitor Network Access Request form at least two (2) business days prior to the day on which the visitor (s) will be on campus and will need access to the network. A form must be completed for each visitor. Visitors and their district department/school sponsor will receive a review from the Richland One Information Technology Administration approving the request to access one of R1's Visitor Access networks. This form **is not** to be completed by the visitor.

**Please note that the use of the district's Internet is not included in the rental agreement through Facilitron. External partners must bring their own hotspots if Internet is needed. **

It is the responsibility of the Departments/School sponsors to ensure their visitor(s) have the R1 Visitor Access to the Internet directions on how to connect to the R1 Visitor Network.

Departments/Schools that will be sponsoring more than ten (10) visitors for an event will need to gather the required information needed (see form for information) on an Excel document and email the **link** the Excel document to **visitors@richlandone.org** at least two (2) business days prior to the day on which the visitors will be on campus and will need access to the network. Access will not be granted to anyone not provided on the list. **Do not send** the attachment to the Excel file. This is so that if any changes need to be made, you can make them in real time and note the changes in red.

Access is only approved for the following reasons:

- Professional learning with a department/school.
- Presentation with a department/school.
- Working with students (student teacher, consultant, guest lecturer, etc.)
- Conducting business with a department/school.

The network is limited in what the visitor can have access to. Some resources that **will not be** unblocked are Google Docs, You Tube, Vimeo, Dropbox, social media sites, other cloud storage sites, etc. ***We are also not able to unblock G-mail, so we encourage visitors to provide district staff with another email address if they need to access their email while on site.***

Access will be monitored on this network at all times. At any time, if malicious traffic is detected, the user will be disconnected from the network and will not be allowed future access. When completing the form, the Richland One staff member who is submitting the form needs to ensure that the name and email address provided is the same that the visitor(s) will provide upon their arrival as that is what is used to authenticate their access when connecting to the network. If access is needed during the weekend and/or after 4:00 pm Monday - Friday, the department/school will be responsible for submitting an Event Support ticket through One to One Plus and paying for a Technology Support Specialist to work the event providing access, as all access is provided in real-time.

USERS THAT HAVE APPLE DEVICES MUST HAVE CHROME DOWNLOADED ON THEIR DEVICES TO ACCESS OUR VISITOR NETWORK.

Note: The Richland One Visitor Wi-Fi network is not available for those that rent district facilities.

Visitors may wish to bring a personal hotspot to ensure that they have access to the resources they may need.

As a reminder, this network is not for staff.

Unscheduled Visitors

Please note that for schools that may have a non-scheduled visitor for an award or other site visit, please contact the Customer Care Center/Help Desk at **80000** immediately after your visitor(s) arrive to provide us with their email address(es). You will need to provide them with a printed copy of the R1 Visitor Access to the Internet directions on how to connect to the R1 Visitor Network. As soon as their email comes through the system their access will be granted.