Technology Considerations for Partnerships, Programs, and Projects with Colleges, Universities, Businesses, and Non-Profit Organizations
April 2, 2019

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

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

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

Considerations
Potential partners must consider the following when proposing projects, programs, activities, software, hardware, or other digital resources for use with students and/or staff in Richland One:

Network
- The District does not create “generic logins” for students, staff members, or partners
- All software to be used on or through the District’s network must be reviewed and tested at least 30 days prior to its anticipated “go-live” date
- All hardware to be connected (wired or wireless) to the District’s network or to be connected to another device that is connected to the District’s network must be reviewed and tested at least 30 days before its anticipated “go-live” date
- The District’s network will not be modified (either hardware, configuration, or connections) to support third-party software or hardware
- The District’s wireless network supports only 5GHz connections (older 2.4GHz devices will not connect)
- Devices not belonging to the District may attach only to guest-access networks with limited bandwidth
- Because the District’s network, as well as the State’s network to which the District’s network connects, are purchased through federal E-Rate funding, the District must comply with E-Rate requirements about prohibiting non-educational use of the network, including the prohibition of individual profit-taking through the use of the District’s network
- Partners that wish to connect to, install software on, or provide access to online resources must work with the District’s IT staff to ensure that those resources are compatible with the District’s network and do not require resources or access that the District cannot provide
Security and Safety

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

Data Access, Storage, Creation, Research, and Disposition

- The district and/or school are the sole and exclusive owners of data collected, stored, shared, or created through the use of all third-party applications, programs, and/or other digital resources
- Access to and use of student and staff data are of considerable concern for the District
- Access to and use of student and staff data are subject to federal and state requirements
- Under federal and state requirements, the District must maintain the security of all its data:
  - Data used for teaching, learning, and operations
  - Data used for research and after the research ends
  - Data provided to third-parties, including software applications
  - Data in the hands of third-parties, including after contractual agreements end
  - Data created during the process of use, analysis, and/or reporting
  - Data kept locally or online
  - Data retention and/or disposition
  - Other data
- Protection from loss of data
  - Backup protocols
  - Offsite backups
- Data containing personally identifiable information about Richland One students or staff may not be stored on any server or other device outside the physical and political borders of the United States
  - Such data may not be subject to access, confiscation, or use outside the laws of the United States
  - Such data must be stored and maintained physically where only the laws of the United States may be applied to access, use, or confiscation or seizure
  - Such data may not be controlled by a company or individual that is not subject to the laws of the United States
Data Used by Online and Cloud-based Applications

- The district and/or school are the sole and exclusive owners of data collected, stored, shared, or created through the use of all third-party applications, programs, and/or other digital resources.
- Currently, most educational resources (like most digital resources for home and business use) are accessed and used online.
- Data required for the successful implementation and management of those resources must be uploaded, typically, to the developer/vendor’s servers (in the cloud).
- Contractual agreements with developers and vendors of those resources must include stipulations about the data required by those resources:
  - The district and/or school are the sole and exclusive owners of data collected, stored, shared, or created through the use of all third-party applications, programs, and/or other digital resources.
  - Identification, collection, and use of the data elements required for successful implementation.
  - Ownership of the data remains with the district and/or school.
  - Storage of and access to the data while in the possession of the developer and/or vendor.
  - Use of the data elements by the software application and the developer/vendor.
  - Inappropriate use of the data elements.
  - New data created through analysis of and reporting from the data.
  - Destruction of the original data, new data, and analytics at the end of the contractual agreement.
  - No data, in any form, whether anonymized or de-identified, may be kept by any third-party developer and/or vendor, without express written consent of the district; no wording within the developer/vendor’s contract can replace the requirement that express written consent is assigned to the developer/vendor only through a specific attachment or addendum to any such contract.
- Data containing personally identifiable information about Richland One students or staff may not be stored on any server or other device outside the physical and/or political borders of the United States.
  - Such data must not be subject to access, use, or confiscation or seizure, outside the laws of the United States.
  - Such data must be stored and maintained physically where only the laws of the United States may be applied to access, use, or confiscation or seizure.
  - Such data may not be controlled by a company or individual that is not subject to the laws of the United States.

Dual-Enrollment Courses with Partner Colleges and Universities

- Richland One partners with several colleges and universities to provide dual-enrollment opportunities for its high school students.
- District-owned laptops used by Richland One students are always protected by the District’s firewall and filtering resources, whether used at school or away from school.
- Students do not have administrative rights to install software on District-owned laptops.
- Some of the dual-enrollment courses may include online content that is blocked on the Richland One network and, as such, is blocked on the student’s District-owned laptop; if the student is using a Richland One laptop, she/he will not be able to access that content.
  - In such cases, the student must 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) for the purpose of completing course requirements.
Rostering Requirements

- For Richland One, specifically, developers/vendors of software applications that require student or staff rostering must provide a turnkey interface that:
  - Defines data elements required for the rostering
  - Provides the query and extraction tool(s) that creates the rostering file
  - Transforms the extracted data into whatever format is required for import into and/or use by the software application
  - Securely transports the data from the district to the developer/vendor’s secure database
  - Imports or makes the data available to the software application
  - Provides whatever daily/nightly data update process is necessary for full implementation of the software application
  - Ensures that the software application functions as expected by the District
- Potential partners should consider the benefits of creating and using SIS plug-ins that can automate the extraction from the student information system
- Potential partners should consider also the benefits of using third-party data management applications that can access and acquire information from the District’s SIS
- Richland One staff should be involved minimally in this process of rostering (minimally refers to confirming the data elements to be used, providing secure access to those data elements, configuring access for the transport of data to the software application)
- The district and/or school are the sole and exclusive owners of data collected, stored, shared, or created through the use of all plug-ins, third-party applications, programs, and/or other digital resources

Conclusion

K-12 partners can access and provide access to many resources to which K-12 districts and schools cannot provide access. This is a major consideration when potential partners begin developing resources to use on school networks or to provide access to online resources.

Districts and schools need partnerships from within the business communities; they solicit such partnerships regularly. Many software applications provide excellent resources for teaching, learning, and operations.

This document is not an all-inclusive list of the factors to be considered in developing partnerships between district and third-party partners. This document is intended to inform potential partners of all kinds that the District and its schools must comply with all the federal and state requirements; thus, there is a need for our partners to consider those requirements as they propose technology-based activities or products. No wording in a partner contract may replace the wording and/or the intent of this document.