Ridgedale Local School District
Technology Governance & Data Privacy Guidelines

Introduction

Ridgedale Local School District recognizes that protecting student and staff data privacy and security is a critical responsibility. The district collects and maintains confidential information related to students, staff, and operations that must be protected in accordance with federal and state laws.

These Technology Governance Guidelines establish clear expectations, responsibilities, and procedures for all staff to ensure that student data is handled securely, used appropriately, and protected from unauthorized access or disclosure.

These guidelines support compliance with laws including FERPA, COPPA, PPRA, CIPA, and Ohio SB29. These guidelines also support and operationalize Board-adopted policies related to data privacy, technology use, and information security.

Purpose

- Define staff responsibilities related to student data privacy and security
- Establish procedures for handling and protecting data
- Ensure consistent and secure use of technology systems
- Promote transparency in how student data is collected and used

Scope

These guidelines apply to all district employees, administrators, students, volunteers, and any individual with access to district data or systems, including contracted third parties and agents of the district.

Data Classification and Regulatory Alignment

Ridgedale Local School District recognizes that data exists in many forms and must be protected accordingly.

Data and information include, but are not limited to:

- Verbal communication (in-person, phone, or other technologies)
- Printed or hard copy documents
- Digital communications (email, text, chat, social media, etc.)
- Data stored or processed on devices (servers, computers, tablets, mobile devices)
- Data stored on internal systems, external media, or cloud-based services

To ensure appropriate protection, data is classified based on sensitivity:

Data Classification Levels

Personally Identifiable Information (PII)
Information that can identify an individual directly or indirectly, including but not limited to:

- Name, date of birth, student ID
- Social Security number
- Educational, medical, financial, or employment records

Confidential Information
Sensitive information requiring strict protection, including:

- Student education records
- Personnel records
- Financial data
- System credentials and access information

Internal Information
Information intended for internal district use only. Unauthorized disclosure may violate:

- Legal requirements
- Contractual obligations
- Copyright protections

Directory Information
Information that may be disclosed under FERPA unless a parent/guardian opts out, including:

- Student name
- Date and place of birth
- Grade level
- Participation in activities and athletics

Public Information
Information approved for public release, such as:

- District communications
- Public reports
- Approved website content

Regulatory Compliance

Ridgedale Local School District complies with all applicable federal and state laws governing data privacy and security. These regulations guide how data is collected, used, shared, and protected:

FERPA (Family Educational Rights and Privacy Act)
Protects the privacy of student education records and requires parental consent for disclosure, with limited exceptions.
http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

CIPA (Children's Internet Protection Act)
Requires the district to implement internet filtering and monitoring to protect students from harmful online content.
http://www.fcc.gov/guides/childrens-internet-protection-act

COPPA (Children's Online Privacy Protection Act)
Restricts the collection of personal information from students under 13 and requires parental consent for online services.
https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

---

PPRA (Protection of Pupil Rights Amendment)
Provides parents with rights regarding surveys and the collection of student information for certain purposes.
https://www2.ed.gov/policy/gen/guid/fpco/ppra/parents.html

HIPAA (Health Insurance Portability and Accountability Act)
Applies to the protection of health-related information when applicable.
http://www.hhs.gov/ocr/privacy/hipaa/understanding/

PCI DSS (Payment Card Industry Data Security Standard)
Applies to the secure handling of payment card data within district operations.
http://www.pcisecuritystandards.org/

The district communicates data privacy practices, parent rights, and the purpose of data collection through annual notices, district policies, and information available on the district website.

Staff Responsibilities and Data Handling Expectations

All Ridgedale Local School District staff are expected to act as responsible stewards of district data. Staff are accountable for maintaining the confidentiality, integrity, and security of all data accessed, created, or stored as part of their job responsibilities.

Personally Identifiable Information (PII), confidential information, and internal data must be protected at all times and must only be accessed, used, or shared by authorized individuals for legitimate educational or operational purposes.

Data Protection and Handling

Staff are required to:

- Ensure that all sensitive data is stored securely and is not accessible to unauthorized individuals
- Access only the data necessary to perform assigned job duties
- Use district-approved systems and secure methods when transmitting or sharing data
- Follow all district policies regarding data access, storage, and sharing

The downloading, uploading, or transfer of PII, confidential, or internal information must be carefully controlled and only conducted using approved systems and procedures.

Physical and Environmental Awareness

Staff must:

- Use secure printing practices when printing sensitive information
- Never leave printed confidential materials unattended
- Properly dispose of documents containing sensitive information (e.g., shredding when required)
- Be aware of their surroundings and avoid discussing confidential information in public or unsecured environments

This includes avoiding conversations involving student or staff information in hallways, public areas, or on cellular devices where information may be overheard.

Account and System Security

Staff are responsible for maintaining the security of their accounts and access credentials. This includes:

- Never sharing usernames or passwords with others (except authorized technology staff for support purposes)
- Logging out of systems or locking devices when unattended
- Protecting access to devices and systems containing sensitive data
- Reporting any suspicious account activity immediately

Incident Reporting

All staff, contractors, and authorized users must immediately report any known or suspected data privacy or security incident, including:

- Unauthorized access to student or staff data
- Accidental disclosure of sensitive information
- Phishing attempts or suspicious emails
- Lost or stolen devices containing district data

Reports should be made to a supervisor and/or the Technology Department immediately so that appropriate action can be taken.

Digital Tool and Software Approval Procedure

Purpose

To ensure that all digital instructional tools and software used within Ridgedale Local School District meet instructional standards and comply with student data privacy laws, including FERPA, COPPA, PPRA, CIPA, and Ohio SB29.

Procedure

All digital tools, applications, and software intended for use with students must be reviewed and approved prior to implementation.

The approval process is as follows:

1. **Building-Level Review (Instructional Need)**
    - Staff members must first submit requests to their **building principal**
    - The principal will review the request to determine instructional value and alignment with district goals
2. **Curriculum Review (Instructional Alignment)**
    - If approved at the building level, the request is forwarded to the **Curriculum Director/Leader**
    - The curriculum office will evaluate alignment with curriculum standards, instructional effectiveness, and redundancy with existing tools
3. **Technology Review (Privacy & Security Compliance)**
    - Following instructional approval, the request is submitted to the **Technology Department**
    - The Technology Department will review the tool to ensure:
        - Student data privacy protections are in place

- Compliance with FERPA, COPPA, and applicable laws
- Appropriate data security practices
- Acceptable terms of service and data collection practices
- No significant cybersecurity risks

Approval and Use

- Only tools that complete the full approval process may be used with students
- Tools that collect, store, or transmit student data **may not be used** without Technology Department approval
- Approved tools may be used for instructional purposes as intended

---

Staff Responsibilities

- Staff must not independently create student accounts or use unapproved applications
- Staff are responsible for submitting requests and following the approval process prior to use
- Staff must discontinue use of any tool that has not been approved

---

Oversight and Compliance

The Technology Department maintains final approval authority to ensure all digital tools meet student data privacy and security requirements.

The district maintains oversight of approved tools to ensure ongoing compliance with applicable laws and district policies.

Data Management

Ridgedale Local School District implements data management practices to ensure the accuracy, integrity, and security of all data systems.

This includes establishing procedures that ensure:

- Data access is aligned with employee roles and job responsibilities
- Staff are trained on data privacy and security expectations
- Data is maintained accurately and securely across all systems

- Digital tools and vendor contracts are reviewed to ensure compliance with data privacy and security standards

Staff are responsible for ensuring that sensitive data is transmitted securely and only through approved district systems. The transmission of student data to approved services (e.g., student information systems, learning management systems) is managed using secure methods established by the Technology Department.

Passwords or sensitive access credentials must never be shared through email or unsecured communication methods. Files containing confidential or restricted information must not be transmitted externally or to third parties without appropriate authorization.

The storage or transfer of confidential data on personal or unapproved devices (e.g., external drives, USB devices, personal cloud storage) is prohibited unless explicitly authorized.

When employment or access to district systems ends, all district data in an individual's possession must be returned, deleted, or destroyed in accordance with district procedures.

Data Security

Ridgedale Local School District regularly monitors and evaluates data security practices to protect against unauthorized access, data loss, or cybersecurity threats.

Data security applies to all forms of data, including:

- Data stored on district devices
- Data stored in cloud-based systems
- Data accessed remotely

Staff are responsible for:

- Ensuring data is stored in secure, district-approved locations
- Following district procedures for remote access and data protection
- Maintaining the same level of data security when accessing systems off-site

When sharing data, staff must:

- Ensure recipients are authorized to access the information
- Limit sharing to only what is necessary for job-related purposes
- Follow professional conduct and confidentiality expectations

Unauthorized access to data, systems, or accounts is strictly prohibited.

All users should understand that district-owned systems and accounts are monitored and that there is no expectation of privacy when using district technology resources in accordance with district policy.

The district follows established records retention and data destruction practices to ensure that data is not retained longer than necessary.

System Security and Access Control

Access to district systems containing student or staff data is restricted based on job responsibilities.

Ridgedale Local School District utilizes role-based access controls to ensure that:

- Staff are granted access only to the data necessary for their role
- Access is reviewed and adjusted as job responsibilities change
- Access is removed promptly when employment or access is no longer required

User accounts are created only after appropriate authorization and are maintained by the Technology Department. When staff leave the district, access to systems is revoked in a timely manner.

All users must:

- Use secure passwords that meet district requirements
- Never share login credentials
- Log out or secure devices when not in use

The district may utilize tools such as directory services, single sign-on (SSO), and access management systems to maintain account security and monitor access.

Access to sensitive data by third-party vendors is limited to approved providers who meet district data privacy and security requirements.

Physical Security

Ridgedale Local School District maintains physical safeguards to protect technology systems and data from unauthorized access, damage, or theft.

This includes:

- Securing servers and network equipment in controlled environments
- Maintaining an inventory of district technology assets
- Monitoring the movement and use of district-owned devices

Staff are responsible for:

- Securing devices when unattended
- Preventing unauthorized access to devices containing sensitive information
- Ensuring devices are not left logged in or accessible to others

The use of unsecured devices or removable media to store or transport sensitive information is discouraged unless approved and properly secured.

District technology equipment must be returned upon request or upon separation from the district.

Malware, Phishing, and Threat Protection

Ridgedale Local School District implements safeguards to protect systems from viruses, malware, phishing, and other cybersecurity threats.

This includes:

- Network filtering and monitoring systems (CIPA compliance)
- Email security and phishing protection
- System updates and patch management
- Endpoint protection on district devices

Staff play a critical role in maintaining security by:

- Recognizing and reporting phishing attempts
- Avoiding suspicious links, downloads, or attachments
- Reporting potential security threats immediately

District Training and Awareness

Ridgedale Local School District is committed to ensuring that all staff understand and fulfill their responsibilities related to student data privacy and security through structured training and ongoing awareness efforts.

All new employees receive training on district technology policies, procedures, and expectations, including confidentiality requirements and the proper handling of student data.

The district utilizes PublicSchoolWORKS to deliver and track required staff training. Through this system, all staff complete **training** covering:

- Federal and state data privacy laws (including FERPA, COPPA, PPRA, CIPA, and Ohio SB29)
- Confidentiality and protection of student information
- Cybersecurity awareness, including phishing and threat prevention
- Appropriate use of district technology systems and digital resources
- Responsibilities related to electronic records and data handling

District administrators and leadership team members receive additional training and updates to ensure continued compliance with evolving data privacy and security requirements.

Completion of required training is monitored and documented through the district's training system to ensure accountability and compliance.

Ongoing reminders, updates, and communications are provided throughout the year to reinforce best practices and address emerging risks related to data privacy and cybersecurity.

Social Media and Digital Communication Guidelines

Ridgedale Local School District recognizes that access to technology and social media provides valuable opportunities for communication, collaboration, and learning. Staff may use digital tools and social media to support instruction, engage with the community, and enhance educational experiences.

At the same time, staff are expected to use these tools responsibly and in a manner that protects student privacy, maintains professional standards, and aligns with district policies.

Professional Expectations

All staff are expected to:

- Follow the same standards of professional conduct online as they do in person
- Use good judgment when posting or sharing information
- Adhere to district Acceptable Use Policies and Technology Governance Guidelines

- Assume that all online activity may be public, regardless of privacy settings

---

Responsible and Ethical Use

When using social media or digital platforms:

- Staff should only represent the district in an official capacity if authorized
- Personal opinions should be clearly identified as such and not attributed to the district
- Communication should remain professional, respectful, and appropriate at all times
- Staff should only discuss topics within their professional role and responsibility

---

Protection of Confidential Information

Staff must not:

- Share or post any confidential or non-public information
- Disclose personally identifiable information (PII) of students, staff, or families
- Share student records, images, or information without appropriate consent

If there is uncertainty about whether information is confidential, staff should treat it as protected and seek guidance.

Privacy and Personal Information

Staff should:

- Avoid sharing personal information that could create safety or security risks
- Protect the privacy of students, families, and colleagues at all times
- Verify the accuracy of information before sharing or reposting

---

Use of Images and Media

- Student images or videos must not be shared without appropriate parent/guardian consent
- Staff should not post images of students or staff without permission
- District branding, logos, and materials should be used appropriately

---

Online Safety and Awareness

Staff are expected to:

- Exercise caution when clicking links or accessing external content
- Be aware of phishing, scams, and malicious content
- Report any suspicious activity or security concerns

Mistakes and Incident Reporting

If a mistake occurs (such as posting sensitive information):

- The content should be corrected or removed immediately
- The issue should be reported to a supervisor or administrator
- Appropriate steps will be taken to minimize any potential impact

---

Digital Citizenship and Conduct

Staff should model appropriate digital behavior by:

- Communicating respectfully and professionally
- Avoiding harassment, bullying, or inappropriate conduct
- Promoting positive and constructive online interactions

Cyberbullying, harassment, or misuse of digital platforms will not be tolerated and may result in disciplinary action.

Acceptable Use of Technology Resources

Use of district technology resources is a privilege, not a right. All users are expected to use district systems in a responsible, ethical, and lawful manner.

Users must:

- Use district-provided accounts and systems for school-related purposes
- Follow all applicable laws and district policies
- Respect intellectual property and copyright laws
- Report inappropriate or unsafe content

Users must not:

- Use technology for illegal, commercial, or unauthorized purposes
- Attempt to bypass security measures or filtering systems
- Access or distribute inappropriate or harmful content
- Install unauthorized software or applications

The district reserves the right to monitor the use of its technology systems to ensure compliance with policies and to maintain system integrity and security.

Compliance and Enforcement

Failure to follow these guidelines may result in disciplinary action, including loss of technology access, employment consequences, or additional legal action as appropriate.

All staff are expected to review and acknowledge these guidelines annually as part of required district training.