NASHUA SCHOOL DISTRICT

Data Governance Plan

May 14, 2020

Committee Members

- Gregory Rodriguez, Director of IT (Co-chair)
- Kristine Smith, Media Specialist (Co-chair)
- Steve Wante, Network Administrator
- Donna Latina, Systems Administrator
- Ian Harvey, Programmer
- Gladys Marcano, Assistant Systems Administrator
- Tanya Ackerman, Assistant Principal
- Daniel Alexander, Assistant Director of Special Education
- Helayne Talbot, Principal
- Anne Altman, Technology Integrator
- Lynda Walsh, Social Studies Teacher

Background of RSA 189:66 -189:68a (HB1612)

- House Bill 1612 passed in June 2018
  - NH DOE uses FERPA, CIPA, and COPPA as guidelines to develop the following:
    - Become fully compliant within a four year period
    - Data privacy for students and staff
    - Developing, maintaining, and enforcing data security standards throughout the Nashua School District (“the District”)
    - Data Governance Plan - this is a living document

Federal Regulatory Compliance

□Children’s Internet Protection Act (CIPA)

□Children’s Online Privacy Protection Act (COPPA)

□Family Educational Rights and Privacy Act (FERPA)

□Health Insurance Portability and Accountability Act (HIPAA)

□Payment Card Industry Data Security Standard (PCI DSS)

□Protection of Pupil Rights Amendment (PPRA)

□Individuals with Disabilities in Education Act (IDEA)

New Hampshire Regulations

□ New Hampshire State RSA - Student and Teacher Information Protection and Privacy

□ NH RSA 189:65 Definitions

□ NH RSA 189:66 Data Inventory and Policies Publication

□ NH RSA 189:67 Limits on Disclosure of Information

□ NH 189:68 Student Privacy

□ NH RSA 189:68-a - Student Online Personal Information

□ New Hampshire Minimum Standards for Privacy and Security of Student and Employee Data

□ New Hampshire State RSA - Right to Privacy:

□ NH RSA 359-C:19 - Notice of Security Breach Definitions

□ NH RSA 359-C:20 - Notice of Security Breach Required

□ NH RSA 359-C:21 - Notice of Security Breach Violation

Purpose

- The District provides faculty, staff, and students with technology to support productivity, research, and education objectives
- The District is also responsible for the creation, collection, storage and destruction of data
- All persons (Data Custodians) who have access to data are required to follow state and federal laws and District policies and procedures
  - Protect PII (Personal Identifiable Information)
- All forms of data should be protected from the following:
  - Accidental or intentional authorized modification, destruction or disclosure throughout the life cycle
  - Including appropriate security of equipment, software, storage practices used to process, store, transmit data and information

What is PII?

Examples of PII include, but are not limited to:

- Name: full name, maiden name, mother’s maiden name, or alias
- Personal identification numbers: social security number (SSN), passport number, driver’s license number, taxpayer identification number, patient identification number, financial account number, or credit card number
- Personal address information: street address, or email address
- Personal telephone numbers
- Biometric data: retina scans, voice signatures, or facial geometry
- Information identifying personally owned property: VIN number or title number

Scope

- All policy, standards, processes and procedures apply to all students, staff in the District, contractual third parties, and volunteers who have access to the District's systems and data.
- This policy applies to:
  - All forms of verbal, written, and technical communications
  - Hard copy data
  - Data stored on electrical devices with storage capacity
  - Removable media or cloud-based storage

Change of Culture

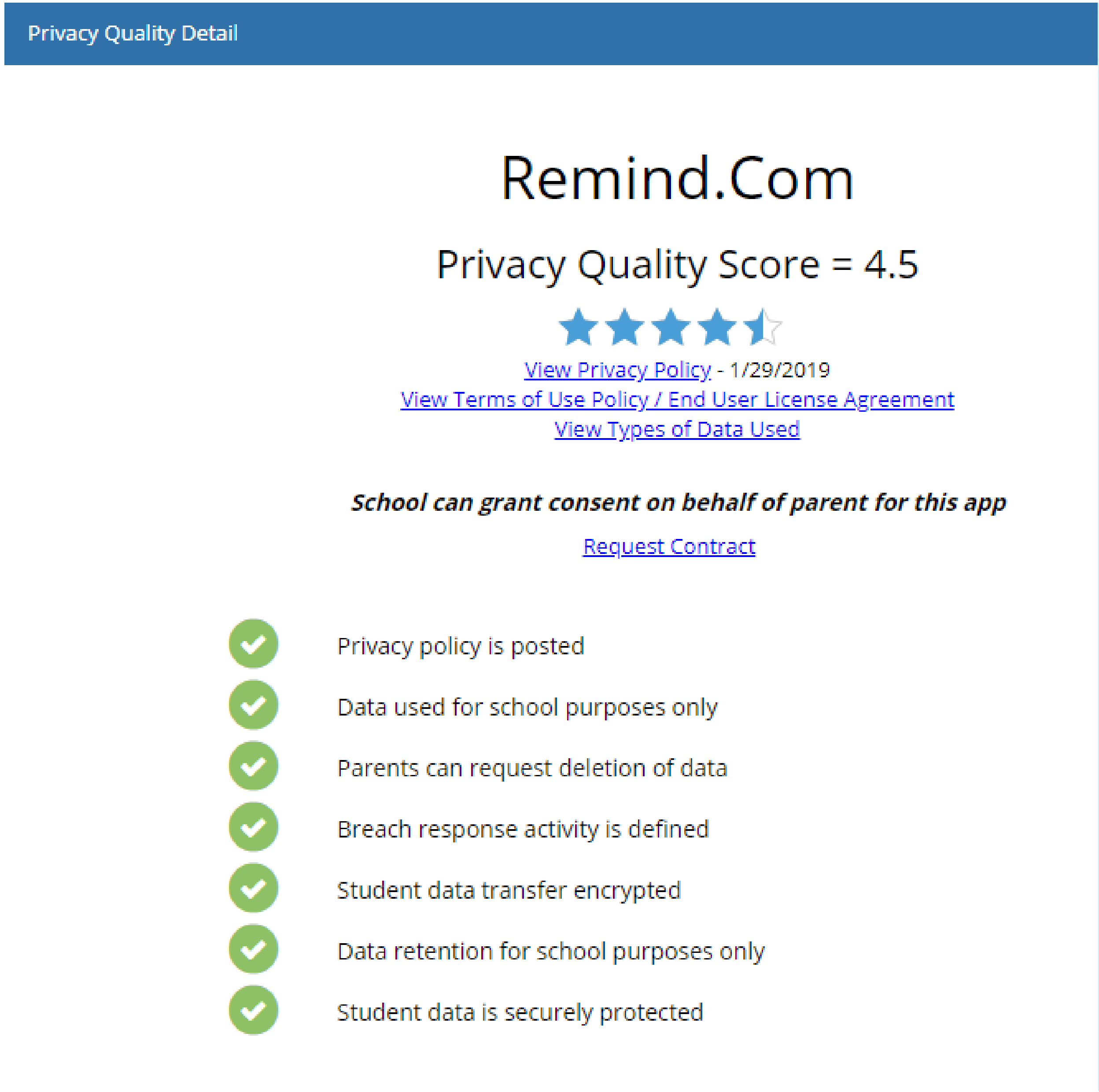
- The spirit of the law requires more restrictive access
  - Safeguard for students and employees
- The District will comply with the standards under the law
- Fostering Digital Citizenship
- Accountability
- This is for the child’s safety
  - Identity
  - Privacy

Data Governance Plan

Appendix Reference	Category
Appendix A	Definitions of terms throughout the plan
Appendix B	Laws, Statutory, and Regulatory Security Requirements
Appendix C	Digital Resource Acquisition and Use
Appendix D	Data Security Checklist
Appendix E	Data Classification Levels
Appendix F	Securing Data at Rest and Transit
Appendix G	Physical Security Controls
Appendix H	Asset Management
Appendix I	Virus, Malware, Spyware, Phishing and SPAM Protection
Appendix J	Account Management
Appendix K	Data Access Roles and Permissions
Appendix L	Password Security
Appendix M	Technology Disaster Recovery Plan
Appendix N	Data Breach Response Plan

Goals - now to end of SY 19-20

- Collect, vet, and inventory all applications, digital tools, and extensions used throughout the District
- Re-examine digital and physical data destruction policy
- Improve IT network and systems to reflect security audit and NIST
- Vet all applications and create Data Privacy Agreement’s (DPA) with vendors through Education Framework (see example).
- Form a Digital Security Awareness Committee to achieve the following:
    - Foster a culture of security and privacy
    - Disseminate best security practices through training and articles
    - Review Data Governance Plan annually



Privacy Quality Detail

Remind.Com

Privacy Quality Score = 4.5

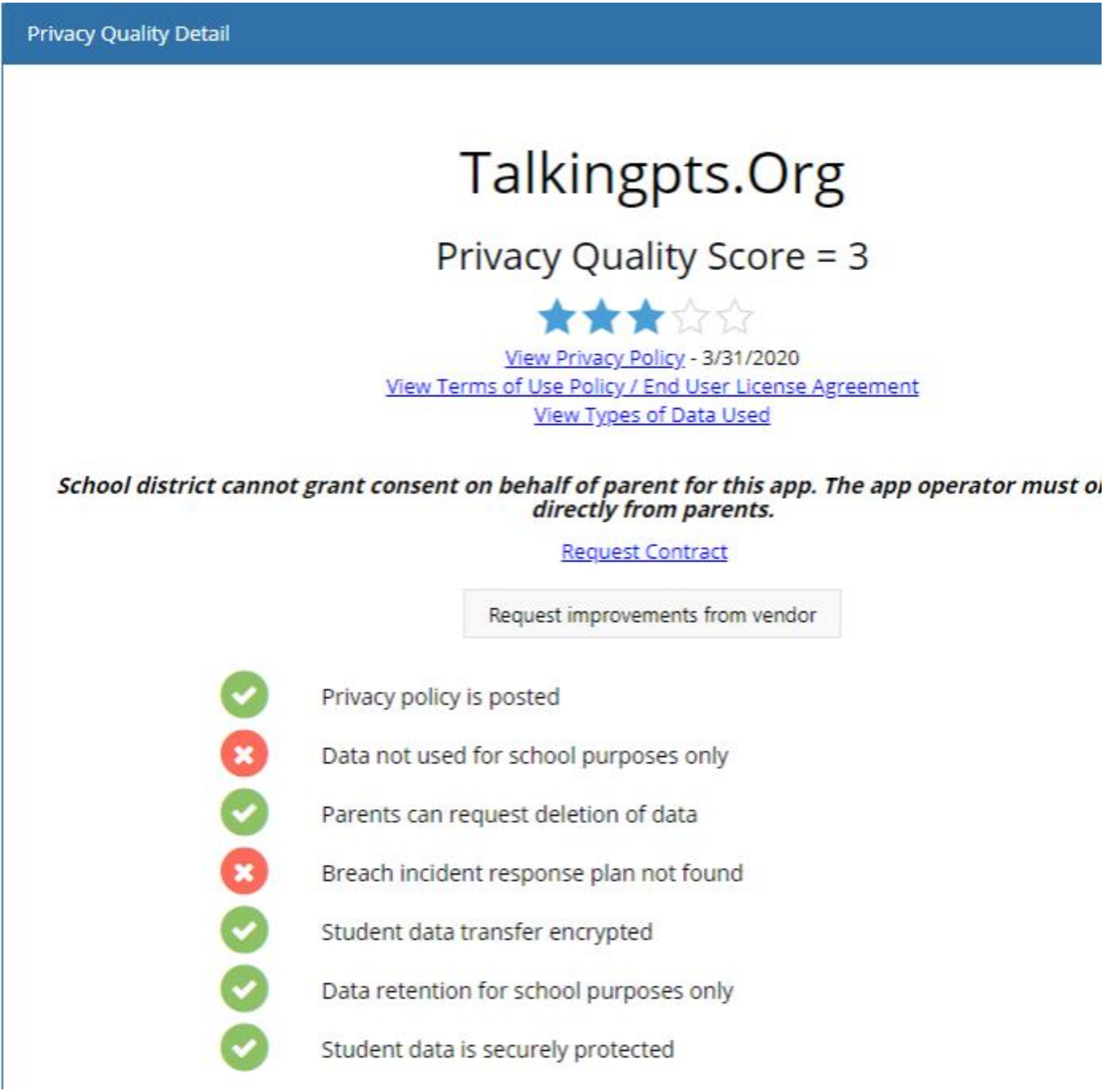
★★★★⯪

View Privacy Policy - 1/29/2019
View Terms of Use Policy / End User License Agreement
View Types of Data Used

School can grant consent on behalf of parent for this app

Request Contract

- ✓ Privacy policy is posted
- ✓ Data used for school purposes only
- ✓ Parents can request deletion of data
- ✓ Breach response activity is defined
- ✓ Student data transfer encrypted
- ✓ Data retention for school purposes only
- ✓ Student data is securely protected



Privacy Quality Detail

Talkingpts.Org

Privacy Quality Score = 3

★★★☆☆

View Privacy Policy - 3/31/2020
View Terms of Use Policy / End User License Agreement
View Types of Data Used

School district cannot grant consent on behalf of parent for this app. The app operator must o directly from parents.

Request Contract

- ✓ Privacy policy is posted
- ✗ Data not used for school purposes only
- ✓ Parents can request deletion of data
- ✗ Breach incident response plan not found
- ✓ Student data transfer encrypted
- ✓ Data retention for school purposes only
- ✓ Student data is securely protected

Goals - beyond 2020

- □ Recompose and rebrand the Responsible User Guide (RUG)
- □ Publish IT Security and Privacy page on the new website
- □ Further refine the process for requesting applications, digital tools, and extensions
- □ Revise and annually present Data Governance Plan to the Nashua Board of Education
- □ Provide on/off-boarding training for employees
- □ Conduct security audit bi-annually