


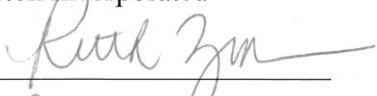
# Addendum #1

The parties to the Snap & Read Universal, Co:Writer Universal Privacy Policy and Terms of Services (“Agreements”), between Don Johnston Incorporated (DJI) and Berlin Public Schools, do hereby add to and amend said Agreement as follows:

DJI warrants that we comply with all Federal Law, including The Family Educational Rights and Privacy Act (FERPA) that protects the privacy of student education records. DJI acknowledges and agrees to fully comply with all provision of Connecticut Law PA16-189. CT PA16-189 provisions take legal precedence over ALL provisions listed in Don Johnston's Privacy Policy, Terms of Service, or any other legal documents, both in existence now or updated in the future. DJI agrees to follow security and breach procedures as described in Appendix 1.

In the event of conflicting provisions between this agreement and the DJI terms and conditions and privacy policy, the DJI terms of service and privacy policy shall control and resolve the conflict. Should a federal, state, county or municipal law or ordinance (“ordinance”) require this agreement to include statements, descriptions or other language, the absence of which will render this agreement invalid, void or unenforceable, DJI will have an opportunity to cure the deficiency should this agreement be challenged on the grounds of omission or non-compliance with ordinance. Once this omission and/or violation is brought to DJI’s attention by a governmental entity, third party, court, counsel or others with the intent or effect that this agreement be invalidated or deemed void, DJI will be given time and opportunity to adopt minimally sufficient required statements, descriptions or other language to maintain the agreement as valid and enforceable. You further agree that upon execution of this agreement any statements, descriptions or other language required by ordinance absent can be retroactively applied with an effective date the same as the original executed agreement at DJI’s discretion or beginning when the statements, descriptions or other language is inserted. DJI will not create statements, descriptions or other language unless required to by ordinance and will likely choose wording that complies with obligations imposed on it with minimal sufficiency. You agree not to challenge any statement, description or additional language incorporated into this agreement or DJI policy that is imposed by ordinance, the continued omission of which can void or invalidate this agreement. You further agree not to challenge the retroactive, present or future effect of the ordinance required statements, descriptions or other language.

Accepted By:  
Berlin Public Schools  
Signature   
Name **Craig E. Szymanski**  
Title **District Technology Coordinator**  
Date **6/4/2018**

Accepted By:  
Don Johnston Incorporated  
Signature   
Name **RUTH ZOLKOWSKI**  
Title **PRESIDENT**  
Date **6/4/2018**

## Appendix 1

### Security Process and Breach Procedures

#### Security Process Management

##### Organizational Safeguards

###### 1. Roles

President: Ruth Ziolkowski

Responsibilities:

Responsible for Company's vision and culture related to Privacy and Security. Provide back-up for Chief Privacy Officers.

Chief Privacy Officer–Software as a Service: Kevin Johnston

Responsibilities:

Responsible for all privacy and security policies and procedures for DJI Services. Lead architecture of services so that we can provide the best privacy and security possible. Monitor COPPA/FERPA and other state legislation in order to meet the needs of our customers and users. Create and monitor Terms of Service and Privacy Policies for our services. Monitor third parties for compliance with policies and procedures. Act as first responder in case of a reported breach for DJI services.

Chief Privacy Officer–Marketing/Sales: Ben Johnston

Responsibilities:

Responsible for all privacy and security policies and procedures for DJI Sales & Marketing. Monitor practices comply with permission marketing. First responder in case of a reported breach for our website/marketing. Responsible for communicating Privacy/Security policies and issues to customers.

Internal IT Systems: Roxine Taylor

Responsibilities:

Internal IT Infrastructure & Systems Management. Contracts with third party annually to audit our IT infrastructure. Responsible for daily monitoring and management of network, servers and systems while implementing periodic security audits and updates. Create procedures for guarding against, detecting, and reporting malicious software/viruses on internal servers and systems.

All Managers

Responsibilities:

Build a culture of security and privacy. Proactively manage department with checks and balances. Ongoing continuing education provided. Reinforce company policies and procedures.

###### 2. Security Awareness and Training

- a. Conducted annually to all staff and third party contractors.
- b. Included in New Employee Orientation Training.

- c. Ongoing security awareness is part of the DJI culture. Managers train as needed within department needs.
- 3. Security Incident Procedures  
See Breach Procedures below
- 4. Human Resource Policies  
Employees sign Confidentiality Agreement as well as Employee Handbook Policy agreements. Policies are aligned and consistent for privacy and security measures. Disciplinary procedures are outlined in Employee Handbook.
- 5. Risk Management/Analysis
  - a. A formal annual risk assessment is conducted every January. Goals include evaluating privacy threats for the organization, business partners and customers. This includes (i) identification of risks to Personally Identifiable Information (PII), (ii) assessing the likelihood and potential damage of such risks, taking into account the sensitivity of the PII (iii) identifying internal and external threats that could result in a Breach and (iv) taking appropriate protection against such
  - b. Informally, risk assessment is ongoing and includes:
    - i. Review key roles and permission levels, policies and separation of duties for checks and balances.
    - ii. Review mitigation controls designed to prevent and detect unauthorized access, theft, or misuse of sensitive data
    - iii. Review security controls, such as encryption of sensitive data in motion and at rest (where feasible);
    - iv. Review data destruction policies, to minimize the risk of data breaches through unauthorized access to archived media or computers that are no longer in use.
- 6. Redundancy and Continuity
  - a. All of our instances are hosted by Amazon Web Services (AWS), which have, at minimum, a 99.95% uptime.
  - b. We use auto scaling to improve availability as instances are scaled up automatically when demand spikes. Impaired instances and/or unhealthy applications are also replaced automatically.
  - c. Application updates and upgrades are deployed with zero downtime.
- 7. Contingency Plan
  - a. Data Backup Plan - Backups are performed at scheduled intervals and stored in geographically discrete regions. They are secured by AWS and are encrypted using the AES-256 algorithm. Access is limited using SSH keys.
  - b. Disaster Recovery Plan & Emergency Mode Operation Plan
    - i. Backups may be restored in geographically discrete regions in the event of a disaster affecting the original region.
    - ii. The tools are also designed, once logged in, to work offline so even server downtime will not affect usage of the tools.
- 8. Work with Third Party Business Associates  
Third Party Associates are expected to:
  - a. Comply with all Security Policies and Procedures.
  - b. Participate in formal annual risk assessment.
  - c. All activity of third party associates is monitored.

## 9. Evaluation

Policy is reviewed annually. Policies are updated as new learnings, procedures and regulations change.

## Technological Safeguards

- a. Location
  - i. All data is located in geographically discrete locations within the United States.
  - ii. AWS hosts all data, and is an ISO 27001 certified provider. In the event that payment is processed online, we use Stripe, a PCI Service Provider Level 1, to process such payments.
- b. Data at Rest - All data at rest is encrypted with AES-256 encryption algorithm.
- c. Data in Transit - All data being transmitted is protected with Secure Socket Layer and password hashing.
- d. DJI Data access
  - i. Access is limited using AWS Identity and Access Management policies.
  - ii. Access is further secured using public-key encryption and/or Two-step authorization.
  - iii. Data access is limited by job roles, and just the essential data to perform one's job functions is made available to individuals.
  - iv. All access is logged.
- e. Incident Investigations
  - i. A Security Information and Event Management (SIEM) overlay is used to investigate and monitor security instances ongoing.
- f. Periodic security audits - Audits are performed on a periodic basis and when:
  1. There are changes in the organization (such as people leaving)
  2. When services are added or removed
  3. When software is added or removed
  4. Whenever suspicions of unauthorized access may have occurred
- g. Lost or Stolen Equipment
  - i. In the event that hardware is lost or stolen, access is managed by AWS Identity and Access Management (IAM), and all access is immediately revoked.
  - ii. No data is ever kept locally or outside of AWS.
  - iii. Logs are kept on all actions and resources accessed. Logs are monitored for any unauthorized access.
  - iv. Security audit will be performed.

## Physical Safeguards

- a. All data is kept on AWS (Amazon) servers.
- b. AWS has the most stringent physical safeguards that has earned it ISO 27001 compliance, a Department of Defense Impact Level 4 Provisional Authorization, over 400 National Institute of Standards and Technology security controls, and a PCI DSS Level 1 certification among other security standards.

## Breach Procedures:

Anyone can report a suspected breach. Services are constantly monitored for breaches. Suspected breaches related to DJI Services are reported directly to the Chief Privacy Officer for Software as a Service. Suspected breaches related to Don Johnston marketing, website are reported directly to the Chief Privacy Officer for Marketing/Sales. This starts the Identification Phase of incident response. The Identification Phase has as its goal the discovery of potential security incidents and the assembly of an incident technical response team that can effectively contain and mitigate the incident.

Once the issue is identified as a breach affecting privacy and information is available, the Chief Privacy Officer will work with the company President and VP of Marketing to communicate both internally and externally. The President will contact and work with our Business Insurance Provider. Individual customers and parents or consumers who have set up accounts directly will be communicated through the web service. Schools who have purchased organizational accounts will have all information directed to the key license contact. To help with communication, we will provide information and language to inform parents.

Chief Privacy Officer and President will also determine whether to notify the authorities/law enforcement (situation dependent) Chief Privacy Officer and President will consult our legal counsel to examine any applicable federal, state, and local breach reporting requirements to determine which additional authorities or entities must be notified in order to satisfy compliance requirements. Chief Privacy Officer and President will seek involvement of law enforcement when there is a reason to believe that a crime has been committed or to maintain compliance with federal, State, or local legal requirements for breach notification. Chief Privacy Officer and President will determine responsibility and roles in communication. Any situation will be added to the Risk Analysis and Mitigation for future policies/procedures for risk mitigation.

