Government of **Western Australia**
Department of **Education**

151 Royal Street, East Perth, Western Australia 6004
Ref: D19/0286086

v3j

*** This questionnaire should be completed in full, questions and formatting should not be edited or amended in any way, and the completed information returned to nigel.hardy@kineticit.com.au as a native spreadsheet with no additional protections or controls in place.**

Queries or issues regarding the completion should be addressed to the email above.

SECTION 1 – GENERAL INFORMATION

Question Number	Category	Question	Response	Additional Details
COM1	Company & Product	Details of authorised person completing this form (name, position and email)		
COM2	Company & Product	Product Name(s) and Version(s)	NoRedInk	
COM3	Company & Product	Purpose and Functionality of Product(s)	Educational Technology - grammar and writing skills development	
COM4	Company & Product	What is your product's licensing model? (E.g. Annual Subscription, One-Time Payment, Ad-Supported, Freeware)	Other - Please provide details	NoRedInk offers a free version of its service and a premium option
COM5	Company & Product	Vendor's Company Name/Legal Entity	NoRedInk Incorporated	
COM6	Company & Product	Registered Company Address	118 2nd Street, San Francisco, CA 94105	
COM7	Company & Product	Vendor's Australian Business/Company Numbers or Country Tax Identifier		
COM8	Company & Product	Total Number of Employees	As of March 2020, we have 93 employees	
COM9	Company & Product	Are you compliant with the Australian Privacy Principles in respect of the in-scope Product	Yes	We believe our privacy practices (https://www.noredink.com/privacy) are consistent with the Australian Privacy Principles
COM10	Company & Product	Does your organisation maintain an Information Security Management System (ISMS)	Yes	Yes via 3rd party. Our product service resides on AWS. As an ISMS, AWS is certified as compliant with ISO 27000. (https://d1.awsstatic.com/certifications/iso_27001_global_certification.pdf)
COM11	Company & Product	Who performs the role of Information Security Manager within your organisation?	Part-time role	Josh Leven
COM12	Company & Product	Who performs the role of Data Privacy Officer/Manager within your organisation?	Part-time role	Josh Leven
COM13	Company & Product	Which of the following policies/standards does your organisation maintain: - Privacy Policy - Computer Usage Policy - Security Policy - Copyright Policy - Access Control Policy - Data Management/Handling Standard - Data Classification Standard - ISO 9001 - ISO 27001	Please reference all that apply with links to published materials and attached soft copies of other documents	Privacy policy (https://www.noredink.com/privacy) Copyright policy (https://www.noredink.com/copyright) Terms of Service (https://www.noredink.com/terms) Access to our our production infrastructure such as applications servers is permission controlled through AWS Identity and Access Manager (IAM) (https://aws.amazon.com/iam) policies. We require engineers to upload ssh access tokens and are able to revoke access centrally for individuals. Password only authentication to these hosts is disabled and access is only possible through use of the access tokens. Database access is limited to users with these tokens by ssh tunnelling through an infrastructure host. There is read access to data in the database for reporting using metabase.io, this access is limited by NoRedInk google credentials.
COM14	Company & Product	Does your organisation maintain the following, or any other documentation and processes in support of business resilience: - Business Continuity Plan - Incident Management/Response Plan - Data Breach Plan	Please reference all that apply with links to published materials and attached soft copies of other documents	We currently do not have documented processes in support of business resilience.
COM15	Company & Product	Do you need to comply with any additional data security or privacy legislation globally, for example, GDPR?	Yes	We currently comply with the Children's Online Privacy and Protection Act (COPPA) and California Consumer Protection Act (CCPA).
COM16	Company & Product	Is your product targeted at school environments? If yes: who are the intended users of the product (e.g. Teachers, Administrative Staff, Students, Parents)?	All of the above	Teachers, students, administrators, parents
COM17	Company & Product	If the product targets Students and/or Minors, are the associated policies, terms and conditions written in a child friendly format?	Yes	Yes, our policies and terms are written in non-legaleze friendly format. In addition, based upon our COPPA alignment, underage and/or minor students

SECTION 2 – SOLUTION INFORMATION

Question Number	Category	Question	Response	Additional Details
SOL1	Solution Architecture	How is your solution architected and hosted?	Third party infrastructure	
SOL2	Solution Architecture	Is any customer or solution data stored offshore to Australia, and if so, in which countries?	Yes - Please list all countries outside of Australia	United States
SOL3	Solution Architecture	Who has physical access to the solution infrastructure and data?	Administrative staff (external/3rd party/service provider)	Our infrastructure is on Amazon Web Services
SOL4	Solution Architecture	How is physical access to the solution environment controlled?	Combination of the above - Please provide details	Amazon has their own procedures for access to the physical servers.
SOL5	Solution Architecture	How do you validate that any third parties, suppliers, vendors and partners that you deal with adhere to the Australian Privacy Principles (https://www.oaic.gov.au/agencies-and-organisations/guides/app-quick-reference-tool), specifically: APP8, APP9 and APP11, and that the third party complies with regulations surrounding Australian Data Sovereignty?	No validation takes place	We believe our privacy practices (https://www.noredink.com/privacy) are consistent with the Australian Privacy Principles (APP). We only choose vendors whose policies are consistent with the obligations of the APP
SOL6	Solution Architecture	Is a mobile app (application) provided for your solution - please specify (IOS, Android, other)?	No mobile app provided	
SOL7	Solution Architecture	Does the solution utilise third party code, services or other resources?	Other - Please provide details	We use both open source and commercial 3rd party solutions.
SOL8	Solution Architecture	How do you manage the security and integrity of third party code and resources?	Not applicable	
SOL9	Solution Architecture	How do you ensure the security of backup data, data on portable devices (including laptops), and data in development and test environments - please include details of security controls including device blocking, encryption, anonymising of data etc?	Other - Please provide details	All client -> server data is transmitted with TLS 1.2 over HTTPS. However, communication between systems in our private network (app servers -> mysql, app servers -> redis, etc.) is unencrypted. PII is not encrypted at rest. Passwords are encrypted at rest using the bcrypt function.
SOL10	Solution Architecture	Does your solution allow you to login and authenticate using an existing social media account (e.g. Facebook, Twitter, Instagram, Google etc.), and are you able to share your solution content directly to a user's social media accounts?	Solution allows login using an existing social media account - Please provide details	Users can login using Google SSO.

SECTION 3 – DATA SECURITY AND PRIVACY INFORMATION

		What type of personal data is utilised and stored by your solution:	*(please select from the below)*	
		Staff and Teachers:		
		Staff Name	Yes	
		Staff Email Address	Yes	
		Staff Personal Information	No	
		Any other staff data (If 'Yes', please provide additional details)		
		Students:		
		Student name	Yes	
		Student home address	No	

DSE1	Data Security and Privacy	*Student telephone number*	No	
		Student email address	Yes	
		Student date of birth	No	
		Student produced work/content	Yes	
		Student attendance records	No	
		Student behavioural records	No	
		Student photos or videos	No	
		Student gender	Yes	
		Student medical or health (inc. mental health) Information	No	
		Student biometric data	No	
		Student geolocation data	No	
		Grades or performance information	Yes	
		Any other student data (If 'Yes', please provide additional details)		
		Parents:		
		Parent name	No	
		Parent contact information	No	
		Any Parent financial or payment data	No	
		Any other parent data (e.g. employment details, reference checks etc.) - If 'Yes' please provide additional details	No	
DSE2	Data Security and Privacy	How do you classify the sensitivity of user and customer data utilised and stored by your solution?	Restricted	
DSE3	Data Security and Privacy	How do you protect data at rest, and in transit - please specify any encryption used, and a summary of your data handling practices?	Encryption - Transit & Rest - Please provide details	In transit, data utilizes SSL encryption. At rest, we utilize Amazon RDS's at rest ecryption solution, Transparent Data Encryption.
DSE4	Data Security and Privacy	How do you control which employees have access to customer and user data within the solution and associated technologies?	Other - Please provide details	While all employees have access to the administrative tools we've built into the product, only engineers, product managers, and specific other employees have direct access to query the database.
DSE5	Data Security and Privacy	Are any of your solution and/or database administration functions outsourced to a 3rd party who may then have access to customer/user data? How is this governed and controlled?	Support/Administration is outsourced - Data access - Please provide details controls in place	We use Amazon Web Services to host and maintain our databases.
DSE6	Data Security and Privacy	How do you secure and protect administrative level access to customer/user data?	Technical controls - Please provide details	We require a username and password associated with an adminstrator account.
DSE7	Data Security and Privacy	Do employees, contractors or other third parties who may access data undergo background and police checks pre and during employment?	No checks are performed	**Is it acceptable that we don't do this?**
DSE8	Data Security and Privacy	What controls do you have in place to prevent unauthorised access to data (either physical or via technical means)?	Technical controls - Please provide details	Access to our our production infrastructure such as applications servers is permission controlled through IAM (https://aws.amazon.com/iam) policies. We require engineers to upload ssh access tokens and are able to revoke access centrally for individuals. Password only authentication to these hosts is disabled and access is only possible through use of the access tokens. Database access is limited to users with these tokens by ssh tunnelling through an infrastructure host. There is read access to data in the database for reporting using metabase.io, this access is limited by NoRedInk google credentials.
DSE9	Data Security and Privacy	What controls do you have in place to prevent copying or theft of data by employees?	No controls in place	**Is it acceptable that we don't do this?**
DSE10	Data Security and Privacy	Is data (identifiable, de-identified or summarised) shared with or sold to any other company, entity, organisation, research body, government department etc., and if so, for what purpose?	Yes - Please provide details	Our privacy policy (https://www.noredink.com/privacy) makes it clear that we will not rent or sell PII. We do share de-identified data with 3rd party services for analysis in support of product maintenance and improvement.
DSE11	Data Security and Privacy	How do you ensure that users, particularly minors, are not exposed to information, advertising or content that can be considered detrimental or of an offensive nature?	We don’t serve advertising within the product but we do use the following services for analysis in support of product maintenance and improvement: Google Analytics MixPanel.com Customer.io Inspectlet.com Rollbar Bugsnag	
DSE12	Data Security and Privacy	If geolocation or biometrics data is collected as part of the provision of the service or product, is this functionality turned **OFF** by default?	Not Applicable	
DSE13	Data Privacy and Access	Do you collect only data that constitutes the minimum possible requirement necessary to operate the service or product, and fully supports the principle of 'data minimisation' under the Australian Privacy Principles?	No - Please provide details	We believe our privacy practices are consistent with the Australian Privcay Principles.
DSE14	Data Privacy and Access	Does your product or service utilise features that ensure 'Privacy by Design' such as enforcing high privacy settings by default (e.g. no unnecessary visibility of other users of the service, marketing and advertising disabled, links to unnecessary services disabled, geolocation and other tracking disabled)?	Yes	Our privacy policy is detailed out here: https://www.noredink.com/privacy. We do not provide unnecessary visibility of other users, we do not market or advertise, or provide links to unnecessary services, we do not perform geolocation of users.
SECTION 4 – LOGGING INFORMATION				
LOG1	Logging	Do you maintain logs of employee access to systems and data, and the activities performed?	Yes - Minimal logging	We use AWS CloudTrail, which gives logs about user access and infrastructure changes. We use GoogleApps, which gives us logs about user access. We have logs from our application servers, database servers, and load
LOG2	Logging	How long are these logs retained?	Logs retained for 90+ days	
LOG3	Logging	Who has access to these logs?	3rd Party and internal administrative staff only	
LOG4	Logging	Do you maintain security incident and event logs?	Yes - Minimal logging (some elements of the solution)	
LOG5	Logging	How long are these security logs retained?	Logs retained for 90+ days	
LOG6	Logging	Who has access to these security logs?	3rd Party and internal administrative staff only	
LOG7	Logging	Do you utilise a SIEM or other monitoring and alerting solution to triage and manage security events and incidents?	Yes - Other - Please provide details	We use AWS CloudTrail and CloudCheckr to help monitor system activity and support triage of security events and incidents. We don't currently have an alerting solution in place.
SECTION 5 – ACCESS AND AUTHENTICATION INFORMATION				
ACC1	Access and Authentication	How does a user authenticate to the solution?	Other - Please provide details	Users can authenticate using a username and password, or an email and password, or use a Single-Sign-On solution: Google SSO or Clever SSO.
ACC2	Access and Authentication	Does the solution provide unique usernames for all users?	Yes - All usernames are unique	
ACC3	Access and Authentication	How do you validate that the user is a legitimate user who should be granted access to the solution, and not an imposter?	No validation takes place	
ACC4	Access and Authentication	How are user accounts managed?	Other - Please provide details	User accounts are managed by the user, but teachers can also manage the accounts of their students.
ACC5	Access and Authentication	How are user credentials secured within the solution?	Encryption - Please provide details	User credentials are encrypted in transit utilizing TLS 1.2 over HTTPS. User credentials are not encrypted at rest.
ACC6	Access and Authentication	Does the solution support role based access?	Role based access (administrator, staff and student accounts)	
ACC7	Access and Authentication	Does the solution support Multi Factor Authentication i.e. MFA, 2FA etc?	No support for MFA	

ACC8	Access and Authentication	Does the solution access other apps on the user's device (computer, smartphone etc.) to deliver supplemental functionality, for example, sending emails, updating a status, or sharing contacts on behalf of the user?	No	
ACC9	Access and Authentication	Are there any age restrictions on the use of the service and are there any parent/guardian consent rules which apply?	Yes - Other - Please provide details	Our privacy policy (https://www.noredink.com/privacy) makes it clear the age restrictions for the use of the NoRedInk service, including parental consent for underage children.
ACC10	Access and Authentication	Does the creation of a user account create a public facing or in-solution browsable profile of that user?	No	
SECTION 6 – SECURITY ASSURANCE INFORMATION				
SEC1	Security Assurance	Do you perform vulnerability assessment across your customer solution and corporate environment?	No testing is performed	
SEC2	Security Assurance	Do you perform penetration testing across your customer solution and corporate environment?	No testing is performed	
SEC3	Security Assurance	Are the results of security assessments made available to consumers of your solution?	Not applicable (testing not performed)	
SEC4	Security Assurance	What is your policy on notifying users of a data breach?	Notification provided <7 days	Our current practice is to notify a client within 48 hours of the recognition of a data breach.
SEC5	Security Assurance	Have your solution or corporate systems ever been subject to a data breach?	No	
SECTION 7 – DATA PRIVACY AND ACCESS INFORMATION				
DAT1	Data Privacy and Access	Who owns data uploaded or created within the product or service	User own all data and content, with limited rights granted to the solution vendor - Please provide details	Our terms of service (https://www.noredink.com/terms) describes our policy of ownership of user submissions. All user submissions belong to the user, however the user grants NoRedInk a license to translate, modify (for technical purposes, for example making sure the content is viewable on an iPhone as well as a computer) and reproduce such user submissions, in each case to enable us to operate the Services. This is a license only – ownership in user submissions is not affected.
DAT2	Data Privacy and Access	What is the process for an individual user to request a copy of their data held by your company?	We are in compliance with CCPA, which requires we have a means to provide and remove a users data from our system. At any time, client may request a copy of their data directly from NoRedInk by submitting a written request via Privacy Request Form (https://preferences.noredink.com/privacy).	
DAT3	Data Privacy and Access	Can users request account closure and complete deletion of their profile and associated data?	Yes, with limitations - Please provide details	We are in compliance with CCPA, which requires we have a means to provide and remove a users data from our system. At any time, client may request a permanent deletion of their data directly from NoRedInk by submitting a written request via a Privacy Request Form (https://preferences.noredink.com/privacy).
DAT4	Data Privacy and Access	How long do you retain backups and archives of user and customer data?	> 1 year	User and customer data are typically retained indefinitely unless a written request for permanent deletion is received from the client.
DAT5	Data Privacy and Access	How long is customer and user data retained for after a user profile is deactivated/deleted?	> 3 months - no backup purge	User and customer data are typically retained indefinitely unless a written request for permanent deletion is received from the client.
DAT6	Data Privacy and Access	Is user or customer data utilised in order to target the sale of additional services or products by yourselves or a third party?	No	

SECTION 8 - EVIDENCE ATTACHED

Please list any evidence supporting the question responses above:

SECTION 9 - DECLARATION

I declare that the information I have provided is true to the best of my knowledge - I have not withheld any relevant information, or made any false or misleading representation.

I hereby give my permission for the responses above to be shared with other education jurisdictions to facilitate the development of a national standard

Name

Position

Signature: (electronic)

Date:

Forward this completed form and relevant evidence to the assessment team via email to nigel.hardy@kineticit.com.au