151 Royal Street, East Perth, Western Australia 6004 Ref: D19/0286086 \* 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 niget.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.

ECTION 1 – GENERAL INFO				
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) a 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 certified as compliant with ISO 27000. (https://dl.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 - Cospyright Policy - Cospyright Policy - Cospyright Policy - Cospyright Policy - Ose of the Cospyrig	Please reference all that apply with links to published materials and attached soft copies of other documents	Privacy policy (https://www.nocelink.com/grinacy). Copyright policy (https://www.nocelink.com/copyright) Terms of Service (https://www.nocelink.com/copyright) Terms of Service (https://www.nocelink.com/terms) Access to our our production infrastructure such as applications servers permission controlled through AVIS lebertly and Access Manager (IAMI) //www.antaon.com/jami policies. We require engineers to upload shis not occess and are able to revoke access centrally for individuals. Production and the reliable revoke access centrally for individuals. Production to these hosts is diabeled and access is only possible through an infrastructure host. There is read access to data in the datable for reporting using metabase io, this access is limited by NoRedink google credentals.
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 A (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. addition, based upon our COPPA alignment, underage and/or minor stu
CTION 2 - SOLUTION INF	ORMATION			
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 serve
SOL5	Solution Architecture	How do you validate that any third parties, suppliers, vendors and partners that you deal with adhere to the Australian Privary Principles (https://www.oaic.gov.au/agencies-and-organisations/guides/apequick-reference-tool), specifically APP6, APP9 and APP11, and that the third party complies with regulations surrounding Australian Data Sovereigngt?	No validation takes place	We believe our privacy practices (https://www.noredink.com/privac 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 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.
CTION 3 - DATA SECURI	TY AND PRIVACY INF	ORMATION		
		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 Staff Personal Information	Yes	
		Staff Personal Information  Any other staff data (If 'Yes', please provide additional details)	No	
		Any other staff data (If 'Yes', please provide additional details)  Students:		
		Students:	Yes	
	1	Student home address	res No	<del> </del>
	1	OLUGOTA HOME BUUTESS	140	

		<del></del>		
		Student telephone number	No	
		Student email address Student date of birth	Yes No	
		Student produced work/content	Yes	
DSE1	Data Security and Privacy	Student attendance records	No	
DSE1	Data Security and Privacy	Student behavioural records	No	
		Student photos or videos	No	
		Student gender	Yes	
		Student medical or health (inc. mental health) Information	No	
		Student biometric data Student geolocation data	No No	
		Grades or performance information	No Yes	
		Any other student data (If 'Yes', please provide additional details)	res	
		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	No	
DSE2	Data Security and Privacy	provide additional details  How do you classify the sensitivity of user and customer data utilised and stored by your	Restricted	
DSE3		solution?		
	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' 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	Other - Please provide details	While all employees have access to the administrative tools we've built
		solution and associated technologies?		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	Support/Administration is outsourced - Data access - Please provide details controls in	We use Amazon Web Services to host and maintain our databases.
	,	party who may then have access to customer/user data? How is this governed and controlled?	place	
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	No checks are performed	Is it acceptable that we don't do this?
		background and police checks pre and during employment?		
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)
		priyacal of via technical means):		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 in 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, do identified or summarised) shared with or sold to any other	Yes - Please provide details	Our privacy policy (https://www.parodink.com/privacy) makes it clear
DSEIU	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	res - 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
		what purpose?		party services for analysis in support of product maintenance and improvement.
DSE11				improvement.
DSETT	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	
			MixPanel.com Customer.io	
			MixPanel.com	
			MixPaneL.com Customer.io Inspectlet.com	
DSE-12	Data Security and Privacy	Washington or hipmatries data is collected as part of the provision of the sender or	MoPanel.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?	MixPanel.com Customer.io Inspectlet.com Rollbar	
		product, is this functionality turned OFF by default?  Do you collect only data that constitutes the minimum possible requirement necessary to	MoPanel.com Customer.io Inspectite.com Rollbur Bugsmag	We believe our privacy gractices are consistent with the Australian Privacy
DSE12 DSE13	Data Security and Privacy  Data Privacy and Access	product, is this functionality turned OFF by default?  Do you collect only data that constitutes the minimum possible requirement necessary to	MoPanel.com Customer.io Inspectlet.com Rollbar Bugsnag	We believe our privacy practices are consistent with the Australian Privacy Principles.
DSE13	Data Privacy and Access	product, is this functionality turned OFF by default?  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?	MoPanel.com Customer.do Inspectitei.com Rollbur Bugsmag	Principles.
		product, is this functionality furned OFF by default?  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?  Des varur mortum is exemine utilise relatives that ensure "Privacy by Design" such as	MoPanel.com Customer.do Inspectitei.com Rollbur Bugsmag	Principles.  Our privacy policy is detailed out here: https://www.noredink.
DSE13	Data Privacy and Access	product, is this functionality furned OFF by default?  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?  Des varur mortum is exemine utilise relatives that ensure "Privacy by Design" such as	MisPaneLcon Customer.io Inspectite.com Rollbar Bugsnag Not Applicable No - Please provide details	Principles.  Our privacy policy is detailed out here: https://www.noredink.com/privacy. We do not provide unnecessary visibility of other users.
DSE13	Data Privacy and Access	product, is this functionality turned OFF by default?  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?	MisPaneLcon Customer.io Inspectite.com Rollbar Bugsnag Not Applicable No - Please provide details	Principles.  Our privacy policy is detailed out here: https://www.noredink.
DSE13	Data Privacy and Access  Data Privacy and Access	product, is this functionality furmed OFF by default?  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 Phinary Principles?  Does your product or service utilities returned that ensure "Phinary 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,	MisPaneLcon Customer.io Inspectite.com Rollbar Bugsnag Not Applicable No - Please provide details	Principles.  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
DSE13	Data Privacy and Access  Data Privacy and Access	product, is this functionality furmed OFF by default?  Do you collect not you than the constitutes the minimum possible requirement necessary to operate the service or product, and fairly supports the principle of data minimisation under the Australian Princey Principle.  Does your product or service utilize features that ensure "Princey by Design" such as errorioning high princy 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.  Do you maintain logs of employee access to systems and data, and the activities	MisPaneLcon Customer.io Inspectite.com Rollbar Bugsnag Not Applicable No - Please provide details	Principles.  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
DSE13  DSE14  SECTION 4 – LOGGING INFOR	Data Privacy and Access  Data Privacy and Access  RMATION	product, is this functionality furmed OFF by default?  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 Phinosy Principles?  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 the service, marketing and advertising the service. The product of the service of the s	MorPanel.com Customer.io Inspectite.com Rollbur Bugsmag Wort Applicable No- Please provide details Yes	Principles.  Our princip policy is detailed out here. https://www.noredrink. comprincip. We do not provide unnecessary visibility of other users, we do not market a defended, or provide links to unnecessary services we do not princip a defended, or provide links to unnecessary services we do not perform geolocalism of users.  We use AWS Cloud Trail, which gives logs about user access and infrastructure changes.
DSE13  DSE14  SECTION 4 – LOGGING INFOR	Data Privacy and Access  Data Privacy and Access  RMATION	product, is this functionality furmed OFF by default?  Do you collect not you than the constitutes the minimum possible requirement necessary to operate the service or product, and fairly supports the principle of data minimisation under the Australian Princey Principle.  Does your product or service utilize features that ensure "Princey by Design" such as errorioning high princy 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.  Do you maintain logs of employee access to systems and data, and the activities	MorPanel.com Customer.io Inspectite.com Rollbur Bugsmag Wort Applicable No- Please provide details Yes	Principles:  Our privacy policy is detailed out here: https://www.noredink.  com/privacy. We do not provide unnecessary visibility of other users, we do not narket or advertise, or provide links to unnecessary services we do not perform geolocation of users.  We use AWS CloudTrail, which gives logs about user access and infrastructure changes.
DSE13  DSE14  SECTION 4 – LOGGING INFOR	Data Privacy and Access  Data Privacy and Access  RMATION  Logging	product, is this functionality furmed OFF by default?  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 Phivacy Principles?  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 labelled, links to unnecessary services disabled, geolocation and other tracking disabled?  Do you maintain logs of employee access to systems and data, and the activities performed?	MorPanel con Customer Jo Customer Jo Rollbar Rollbar Not Applicable No - Please provide details Yes  Yes - Minimal logging	Principles.  Our princip policy is detailed out here. https://www.noredrink. comprincip. We do not provide unnecessary visibility of other users, we do not market a defended, or provide links to unnecessary services we do not princip a defended, or provide links to unnecessary services we do not perform geolocalism of users.  We use AWS Cloud Trail, which gives logs about user access and infrastructure changes.
DSE13  DSE14  SECTION 4 - LOGGING INFOR LOG1  LOG2	Data Privacy and Access  Data Privacy and Access  RMATION Logging  Logging	product, is this functionality furmed OFF by default?  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 Phinacy Principles?  Does your product or service utilise features that ensure "Prinacy by Design" such as enforcing high privacy settings by default (e.g. no unnecessary visibility of other users of the service, marketing and advertising liabelled, links to unnecessary services disabled, geolocation and other tracking disabled)?  Do you maintain logs of employee access to systems and data, and the activities performed?  How long are these logs retained?	MorPanel con Customer io Customer io Bolloar Bolloar Bolloar Bolloar No - Please provide details Yes Yes - Minimal logging Logs retained for 90+ days	Principles:  Our privacy policy is detailed out here: https://www.noredink.  com/privacy. We do not provide unnecessary visibility of other users, we do not narket or advertise, or provide links to unnecessary services we do not perform geolocation of users.  We use AWS CloudTrail, which gives logs about user access and infrastructure changes.
DSE13  DSE14  SECTION 4 - LOGGING INFOR	Data Privacy and Access  Data Privacy and Access  RMATION  Logging	product, is this functionality furmed OFF by default?  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 Phivacy Principles?  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 labelled, links to unnecessary services disabled, geolocation and other tracking disabled?  Do you maintain logs of employee access to systems and data, and the activities performed?	MorPanel con Customer Jo Customer Jo Rollbar Rollbar Not Applicable No - Please provide details Yes  Yes - Minimal logging	Principles:  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.  We use AWS CloudTrail, which gives logs about user access and infrastructure changes.
DSE13  DSE14  SECTION 4 - LOGGING INFOR  LOG1  LOG2	Data Privacy and Access  Data Privacy and Access  RMATION Logging  Logging	product, is this functionality furmed OFF by default?  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 Phinacy Principles?  Does your product or service utilise features that ensure "Prinacy by Design" such as enforcing high privacy settings by default (e.g. no unnecessary visibility of other users of the service, marketing and advertising liabelled, links to unnecessary services disabled, geolocation and other tracking disabled)?  Do you maintain logs of employee access to systems and data, and the activities performed?  How long are these logs retained?	MorPanel con Customer io Customer io Bolloar Bolloar Bolloar Bolloar No - Please provide details Yes Yes - Minimal logging Logs retained for 90+ days	Principles:  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.  We use AWS CloudTrail, which gives logs about user access and infrastructure changes.
DSE13  DSE14  SECTION 4 - LOGGING INFOR  LOG2  LOG2  LOG3	Data Privacy and Access  Data Privacy and Access  RMATION Logging  Logging  Logging	product, is this functionality furmed OFF by default?  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?  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, inks to unnecessary services disabled, geolocation and other tracking disabled)?  Do you maintain logs of employee access to systems and data, and the activities performed?  How long are these logs retained?  Who has access to these logs?	MorPanel con Customer io Customer io Registration Registration Registration Rollbar Ro	Principles:  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.  We use AWS CloudTrail, which gives logs about user access and infrastructure changes.
DSE13  DSE14  SECTION 4 - LOGGING INFOR  LOG2  LOG2  LOG3  LOG4  LOG5	Data Privacy and Access  Oata Privacy and Access  RMATION Logging Logging Logging Logging Logging Logging	product, is this functionality furned OFF by default?  Do you collect not you than the constitutes the minimum possible requirement necessary to operate the service or product, and fully supports the principle of data minimisation under the Australian Princey Principle.  Does your product or service utilize features that ensure Princey by Design's such as erroricing high princy settings by default (e.g. no unnecessary visibility of other users of the service, marketing and advertising disabled, links to unnecessary services disabled, geolocitation and other tracking disabled.  Do you maintain logs of employee access to systems and data, and the activities performed?  Who has access to these logs retained?  Who has access to these logs?  Do you maintain security incident and event logs?  How long are these security logs retained?	MorPanel con Customer Jo Inspectific Com Bugsrag  No - Please provide details  Yes  Yes - Minimal logging  Logs retained for 90+ days  3rd Party and internal administrative staff only Yes - Minimal logging (some elements of the solution)  Logs retained for 90+ days	Principles:  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.  We use AWS CoudTrail, which gives logs about user access and infrastructur changes.  We use AWS CoudTrail, which gives logs about user access and infrastructur changes.
DSE13  DSE14  SECTION 4 - LOGGING INFOR  LOG2  LOG3  LOG4  LOG5  LOG6	Data Privacy and Access Data Privacy and Access  MATION Logging Logging Logging Logging Logging Logging Logging	product, is this functionality furned OFF by default?  Do you colled not yolds that cursuits he harminum possible requirement necessary to operate the service or product, and fully supports the principle of data minimisation under the Australian Princey Principle.  Does your product or service utilise features that ensure Princey by Design's such as errorioning high princy settings by default (e.g. no unnecessary visibility of other users of the service, marketing and advertising disabled, links to unnecessary services disabled, geolocitation and other tracking disabled, links to unnecessary services disabled, geolocitation and other tracking disabled, and the activities performed?  Do you maintain logs of employee access to systems and data, and the activities performed?  Who has access to these logs?  Do you maintain security incident and event logs?  How long are these security logs retained?  Who has access to these security logs retained?	MorPanel con Customer Jo Inspectific Com Bugurag  No - Please provide details  No - Please provide details  Yes  Yes - Minimal logging  Logs retained for 90+ days  3rd Party and internal administrative staff only  Yes - Minimal logging (some elements of the solution)  Logs retained for 90+ days  3rd Party and internal administrative staff only	Principles:  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.  We use AWS CloudTrail, which gives logs about user access and infrastructur changes.  We use AWS CloudTrail, which gives logs about user access. We have logs from our application servers, database servers, and load
DSE13  DSE14  SECTION 4 - LOGGING INFOR  LOG1  LOG2  LOG3  LOG4  LOG5	Data Privacy and Access  Oata Privacy and Access  RMATION Logging Logging Logging Logging Logging Logging	product, is this functionality furned OFF by default?  Do you colled only date that constitutes the minimum possible requirement necessary to under the Australian Privacy Principle ("poports the principle of data minimisation" under the Australian Privacy Principle ("poports the principle of data minimisation" under the Australian Privacy Product of service utilise features that crears "Privacy by Design" such as considered that the principle of the privacy by Design such as the service, marketing and advertising disabled, links to unnecessary services disabled, seolocation and other tracking disabled, links to unnecessary services disabled, seolocation and other tracking disabled, links to unnecessary services disabled, seolocation and other tracking disabled, links to unnecessary services disabled, seolocation and other tracking disabled, links to unnecessary services disabled, seolocation and other tracking disabled, links to unnecessary services disabled, seolocation and other tracking disabled. The properties of the service of the serv	MorPanel con Customer Jo Inspectific Com Bugsrag  No - Please provide details  Yes  Yes - Minimal logging  Logs retained for 90+ days  3rd Party and internal administrative staff only Yes - Minimal logging (some elements of the solution)  Logs retained for 90+ days	Principles:  Our privacy policy is detailed out here: https://www.noredink.  Comprivacy. We do not provide unnecessary visibility of other users, we do not narket or advertise, or provide links to unnecessary services we do not perform geolocation of users.  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  We use GoogleApps, which gives us logs about user access.  We have logs from our application servers, database servers, and load
DSE13  DSE14  SECTION 4 – LOGGING INFOR  LOG1  LOG2  LOG3  LOG4  LOG5  LOG6  LOG7	Data Privacy and Access  Data Privacy and Access  EMATION Logging Logging Logging Logging Logging Logging Logging Logging Logging	product, is this functionality turned OFF by default?  Do you collect only data that constitutes the minimum possible requirement necessary to governate the service or product, and fully supports the principle of data minimisation?  Does your product or service utilise features that ensure 'Privary by Design' such as enforcing high privary settings by default (e.g. no unnecessary visibility of other cent of geolocation and other tracking disabled). Inks to unnecessary services disabled, geolocation and other tracking disabled, this to unnecessary services disabled.  Do you maintain logs of employee access to systems and data, and the activities performed?  Who has access to these logs?  Do you maintain security incident and event logs?  How long are these security incident and event logs?  Do you tallies a SIEM or other monitoring and alerting solution to triage and manage security events and incidents?	MorPanel con Customer Jo Inspectific Com Bugurag  No - Please provide details  No - Please provide details  Yes  Yes - Minimal logging  Logs retained for 90+ days  3rd Party and internal administrative staff only  Yes - Minimal logging (some elements of the solution)  Logs retained for 90+ days  3rd Party and internal administrative staff only	Principles:  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 gelocization of users when the provide interest to unnecessary services we do not perform gelocization of users when the provide links to unnecessary services we do not perform gelocization of users when the provided links to unnecessary services when the provided links are served infrastructure changes.  We use CoogleApps, which gives us logs about user access.  We have logs from our application servers, database servers, and load
DSE13  DSE14  SECTION 4 - LOGGING INFOR  LOG1  LOG2  LOG3  LOG4  LOG5  LOG6  LOG7  SECTION 5 - ACCESS AND ALL  DSE13	Data Privacy and Access  Data Privacy and Access  MATION Logging	product, is this functionality furned OFF by default?  Do you colled not you fast 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 Project of the service of the service of the service of the service of the service, marketing and advertising disabled, links to unnecessary services disabled, geolocation and other tracking disabled, links to unnecessary services disabled, geolocation and other tracking disabled, links to unnecessary services disabled, geolocation and other tracking disabled, links to unnecessary services disabled, geolocation and other tracking disabled, links to unnecessary services disabled, geolocation and other tracking disabled, links to unnecessary services disabled, geolocation and other tracking disabled, links to unnecessary services disabled, geolocation and other tracking disabled, links to unnecessary services disabled, geolocation and other tracking disabled, links to unnecessary services disabled, geolocation and other tracking disabled, links to unnecessary visitive, and the services disabled, geolocation and other tracking disabled, links to unnecessary visitive, and the second programment of the services and disabled, links to unnecessary visitive, and the services disabled, geolocation and details and the activities performed?  Who has access to these security logs?  Do you maintain security incident and event logs?  Who has access to these security logs?  Who has access to these security logs?  Os will see a SIEM or other monitoring and alerting solution to triage and manage security vents and incidents?	MorPanel con Customer Jo Inspectific Com Bugurag  Not Applicable  No - Please provide details  Yes  Yes - Minimal logging  Logs retained for 90+ days  3rd Party and internal administrative staff only  Yes - Minimal logging (some elements of the solution)  Logs retained for 90+ days  3rd Party and internal administrative staff only  Yes - Other - Please provide details	Principles:  Our privacy policy is detailed out here: https://www.noredink.  Our 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 market or advertise, or provide links to unnecessary services we do not perform geolocation of users we do not perform geolocation of users when the control of the con
DSE13  DSE14  SECTION 4 – LOGGING INFOR  LOG1  LOG2  LOG3  LOG4  LOG5  LOG6  LOG6  LOG7	Data Privacy and Access  Data Privacy and Access  RMATION Logging	product, is this functionality turned OFF by default?  Do you collect only data that constitutes the minimum possible requirement necessary to governate the service or product, and fully supports the principle of data minimisation?  Does your product or service utilise features that ensure 'Privary by Design' such as enforcing high privary settings by default (e.g. no unnecessary visibility of other cent of geolocation and other tracking disabled). Inks to unnecessary services disabled, geolocation and other tracking disabled, this to unnecessary services disabled.  Do you maintain logs of employee access to systems and data, and the activities performed?  Who has access to these logs?  Do you maintain security incident and event logs?  How long are these security incident and event logs?  Do you tallies a SIEM or other monitoring and alerting solution to triage and manage security events and incidents?	MorPanel con Customer Jo Inspectific Com Bugurag  No - Please provide details  No - Please provide details  Yes  Yes - Minimal logging  Logs retained for 90+ days  3rd Party and internal administrative staff only  Yes - Minimal logging (some elements of the solution)  Logs retained for 90+ days  3rd Party and internal administrative staff only	Principles:  Our privacy policy is detailed out here: https://www.noredink.  Our privacy policy is detailed out here: https://www.noredink.  comprivacy. We do not provide unnecessary visibility of other users, we do not market or advertise, or provide links bunnecessary services we do not perform geolocitation of users do not perform geolocitation of user do not perform geolocitation of users.  We use AVS CloudTrail, which gives logs about user access and infrastructure changes.  We have logs from our application servers, database servers, and load  We use AVIS CloudTrail and CloudCheedr to help monitor system solving and support triage of security events and incidents. We don't currently have an alerting solution in place.  Users can authenticate using a username and password, or an email
DSE13  DSE14  SECTION 4 - LOGGING INFOR  LOG2  LOG3  LOG4  LOG5  LOG6  LOG7  SECTION 5 - ACCESS AND ALL  ACCT	Data Privacy and Access  Data Privacy and Access  MATION Logging	product, is this functionality furned OFF by default?  Do you colled not you than the constitutes the minimum possible requirement necessary to operate the service or product, and fully supports the principle of data minimisation under the Australian Principle not the principle of data minimisation under the Australian Principle not the principle of data minimisation under the Australian Principle not produce the service.  Does your product or service utilise features that ensure Principle you besign such as erroricing high principle data devertising disabled, links to unnecessary services disabled, selecication and other tracking disabled. Links to unnecessary services disabled, selecication and other tracking disabled.  Do you maintain logs of employee access to systems and data, and the activities performed?  Who has access to these logs?  Do you maintain security incident and event logs?  How long are these logs retained?  Who has access to these security logs retained?  Who has access to these security logs retained?  Who has access to these security logs?  Do you utilize a SIEM or other monitoring and alerting solution to triage and manage security events and incidents?  ORNATION  How does a user authenticate to the solution?	MorPanel con Customer Jo Integeredic Com Buggeredic No - Please provide details No - Please provide details Yes  Ves - Minimal logging Logs retained for 90+ days 3rd Party and internal administrative staff only Yes - Minimal logging (some elements of the solution) Logs retained for 90+ days 3rd Party and internal administrative staff only Yes - Other - Please provide details Other - Please provide details	Principles:  Our privacy policy is detailed out here: https://www.noredink.  Our 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 market or advertise, or provide links to unnecessary services we do not perform geolocation of users we do not perform geolocation of users when the control of the con
DSE13  DSE14  SECTION 4 - LOGGING INFOR  LOG1  LOG2  LOG3  LOG4  LOG5  LOG6  LOG7  SECTION 5 - ACCESS AND ALL  DSE13	Data Privacy and Access  Data Privacy and Access  MATION Logging Logging Logging Logging Logging Logging Logging Logging Logging Access and Authentication Access and Access and	product, is this functionality furned OFF by default?  Do you colled not you fast 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 Project of the service of the service of the service of the service of the service, marketing and advertising disabled, links to unnecessary services disabled, geolocation and other tracking disabled, links to unnecessary services disabled, geolocation and other tracking disabled, links to unnecessary services disabled, geolocation and other tracking disabled, links to unnecessary services disabled, geolocation and other tracking disabled, links to unnecessary services disabled, geolocation and other tracking disabled, links to unnecessary services disabled, geolocation and other tracking disabled, links to unnecessary services disabled, geolocation and other tracking disabled, links to unnecessary services disabled, geolocation and other tracking disabled, links to unnecessary services disabled, geolocation and other tracking disabled, links to unnecessary visitive, and the services disabled, geolocation and other tracking disabled, links to unnecessary visitive, and the second programment of the services and disabled, links to unnecessary visitive, and the services disabled, geolocation and details and the activities performed?  Who has access to these security logs?  Do you maintain security incident and event logs?  Who has access to these security logs?  Who has access to these security logs?  Os will see a SIEM or other monitoring and alerting solution to triage and manage security vents and incidents?	MorPanel con Customer Jo Inspectific Com Bugurag  Not Applicable  No - Please provide details  Yes  Yes - Minimal logging  Logs retained for 90+ days  3rd Party and internal administrative staff only  Yes - Minimal logging (some elements of the solution)  Logs retained for 90+ days  3rd Party and internal administrative staff only  Yes - Other - Please provide details	Principles:  Our privacy policy is detailed out here: https://www.noredink.  Our privacy policy is detailed out here: https://www.noredink.  comprivacy. We do not provide unnecessary visibility of other users, we do not market or advertise, or provide links to unnecessary service we do not perform geolocation of user do not perform geolocation of user do not perform geolocation of users.  We use AVS CloudTrail, which gives logs about user access and infrastructured target.  We use AVS CloudTrail which gives logs about user access. We have logs from our application servers, database servers, and load  We use AVS CloudTrail and CloudCheder to help monitor system serving and support triage of security events and incidents. We don't currently have an allerting solution in place.  Users can authenticate using a username and password, or an email
DSE13  DSE14  SECTION 4 - LOGGING INFOR  LOG2  LOG3  LOG4  LOG5  LOG6  LOG7  SECTION 5 - ACCESS AND ALL  ACCT	Data Privacy and Access  Data Privacy and Access  MATION Logging Logging Logging Logging Logging Logging Logging Logging Access and Authentication Access and	product, is this functionality furned OFF by default?  Operation the service of the the constitutes the minimum possible requirement necessary to operate the service or product, and fully supports the principle of data minimisation under the Australian Privacy Principle.  Deer your product or service utilise features that ensure "Privacy by Design" such as confercing high privacy settings by default (e.g. as unnecessary visibility of other users of the service, marketing and advertising disabled, links to unnecessary services disabled, seolocation and other tracking disabled, links to unnecessary services disabled, seolocation and other tracking disabled, links to unnecessary services disabled, seolocation and other tracking disabled, links to unnecessary services disabled, seolocation and other tracking disabled.  Do you maintain logs of employee access to systems and data, and the activities performed?  Who has access to these logs?  Do you maintain security incident and event logs?  How long are these security logs retained?  Who has access to these security logs?  Do you utilise a SIEM or other monitoring and alerting solution to triage and manage security events and incidents?  ORMATION  Does the solution provide unique usernames for all users?  How does a user authenticate to the solution?	MorPanel con Customer Jo Integeredic Com Buggeredic No - Please provide details No - Please provide details Yes  Ves - Minimal logging Logs retained for 90+ days 3rd Party and internal administrative staff only Yes - Minimal logging (some elements of the solution) Logs retained for 90+ days 3rd Party and internal administrative staff only Yes - Other - Please provide details Other - Please provide details	Principles:  Our privacy policy is detailed out here: https://www.noredink.  Our privacy policy is detailed out here: https://www.noredink.  comprivacy. We do not provide unnecessary visibility of other users, we do not market or advertise, or provide links to unnecessary service we do not perform geolocation of user do not perform geolocation of user do not perform geolocation of users.  We use AVS CloudTrail, which gives logs about user access and infrastructured target.  We use AVS CloudTrail which gives logs about user access. We have logs from our application servers, database servers, and load  We use AVS CloudTrail and CloudCheder to help monitor system serving and support triage of security events and incidents. We don't currently have an allerting solution in place.  Users can authenticate using a username and password, or an email
DSE13  DSE14  SECTION 4 - LOGGING INFOR  LOG1  LOG2  LOG3  LOG4  LOG5  LOG6  LOG7  SECTION 5 - ACCESS AND AL  ACC1  ACC2  ACC3	Data Privacy and Access  Data Privacy and Access  MATION Logging Access and Actherification Access and Actherification Access and Actherification	product, is this functionality turned OFF by default?  Do you colled not yolds that cursuits he in minimum possible requirement necessary to operate the service or product, and fully supports the principle of data minimisation under the Australian Princey Principle.  Does your product or service utilise features that ensure Princey by Design's such as errorizing high principle and advertising disabled, links to unnecessary services disabled, geolocitation and other tracking disabled, links to unnecessary services disabled, geolocitation and other tracking disabled, links to unnecessary services disabled, geolocitation and other tracking disabled, links to unnecessary services disabled, geolocitation and other tracking disabled, links to unnecessary services disabled, geolocitation and other tracking disabled, links to unnecessary visable, of other users of the service, marketing and generalized services and data, and the activities performed?  Do you maintain logs of employee access to systems and data, and the activities performed?  Who has access to these logs?  Do you maintain security incident and event logs?  How long are these security logs retained?  Who has access to these security logs?  Do you utilise a SIEM or other monitoring and alerting solution to triage and manage security events and incidents?  ORMATION  Does the solution provide unique usernames for all users?  How do you validate that the user is a legitimate user who should be granted access to the solution, and not an imposter?	MorPanel con Customer Jo Inspectific Com Bugurag  No - Please provide details  Yes  Yes - Minimal logging  Yes - Other - Please provide details	Principles:  Our privacy policy is detailed out here: https://www.noredink.  Our 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 when the provide into the provide into the provide into the privacy of the pri
DSE13  DSE14  SECTION 4 – LOGGING INFOR  LOG1  LOG2  LOG3  LOG4  LOG5  LOG6  LOG7  SECTION 5 – ACCESS AND AL  ACC2  ACC3  ACC3	Data Privacy and Access  Data Privacy and Access  MATION Logging Logging Logging Logging Logging Logging Logging Logging Logging Access and Authentication Access and Acthenication Access and Acthenication Access and Acthenication Access and Acthenication Access and Authentication Access and Authentication Access and Authentication	product, is this functionality turned OFF by default?  Do you colled not yolds that customistics the minimum possible requirement necessary to operate the service or product, and fully supports the principle of data minimisation under the Australian Privacy Program of the principle of data minimisation under the Australian Privacy Program of the privacy of the service, analysis of the service, marketing and advertising disabled, links to unnecessary services disabled, geolocitation and other tracking disabled, links to unnecessary services disabled geolocitation and other tracking disabled, links to unnecessary services disabled, geolocitation and other tracking disabled, links to unnecessary services disabled, geolocitation and other tracking disabled, links to unnecessary services disabled, geolocitation and other tracking disabled, links to unnecessary services disabled, geolocitation and other tracking disabled, links to unnecessary services disabled, geolocitation and other tracking disabled, links to unnecessary services disabled, geolocitation and the activities performed?  Who has access to these logs?  Do you maintain security incident and event logs?  How long are these security logs retained?  Who has access to these security logs?  Do you usilistie as SIEM or other monitoring and alerting solution to triage and manage security events and incidents?  ORMATION  ORMATION  Does the solution provide unique usernames for all users?  How do you validate that the user is a legitimate user who should be granted access to the solution, and not an imposter?  How do you validate that the user is a legitimate user who should be granted access to the solution, and not an imposter?	MorPanel con Customer Jo Inspectific Com Bugurag  No - Please provide details  Yes  - Minimal logging  Yes - Minimal logging  Yes - Minimal logging  Yes - Minimal logging  Yes - Minimal logging  Yes - Minimal logging  Yes - Minimal logging (some elements of the solution)  Logs retained for 90+ days  3rd Party and internal administrative staff only  Yes - Other - Please provide details  Other - Please provide details  Other - Please provide details  No validation takes place  Other - Pease provide details	Principles:  Our privacy policy is detailed out here: https://www.noredink.  Our 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 when the privacy is the privacy of the provide into the provide into the privacy we do not perform geolocation of users.  We use AWS CloudTrail, which gives logs about user access and infrastructur changes.  We use GogleApps, which gives logs about user access.  We have logs from our application servere, database servers, and load  We use AWS CloudTrail and CloudChecks to help monitor system activity and support triage of security events and incidents. We don't currently have an altering solution in place.  Users can authenticate using a username and password, or an email expansion of use a Single-Sign-On solution: Coogle SSO or Cleve SSO.
DSE13  DSE14  DSE14  SECTION 4 - LOGGING INFOR  LOG1  LOG2  LOG3  LOG4  LOG5  LOG6  LOG7  SECTION 5 - ACCESS AND AI  ACC1  ACC2  ACC3	Data Privacy and Access  Data Privacy and Access  MATION Logging Logging Logging Logging Logging Logging Logging Logging Access and Authentication	product, is this functionality turned OFF by default?  Do you colled not yolds that cursuits he in minimum possible requirement necessary to operate the service or product, and fully supports the principle of data minimisation under the Australian Princey Principle.  Does your product or service utilise features that ensure Princey by Design's such as errorizing high principle and advertising disabled, links to unnecessary services disabled, geolocitation and other tracking disabled, links to unnecessary services disabled, geolocitation and other tracking disabled, links to unnecessary services disabled, geolocitation and other tracking disabled, links to unnecessary services disabled, geolocitation and other tracking disabled, links to unnecessary services disabled, geolocitation and other tracking disabled, links to unnecessary visable, of other users of the service, marketing and generalized services and data, and the activities performed?  Do you maintain logs of employee access to systems and data, and the activities performed?  Who has access to these logs?  Do you maintain security incident and event logs?  How long are these security logs retained?  Who has access to these security logs?  Do you utilise a SIEM or other monitoring and alerting solution to triage and manage security events and incidents?  ORMATION  Does the solution provide unique usernames for all users?  How do you validate that the user is a legitimate user who should be granted access to the solution, and not an imposter?	MorPanel con Customer Jo Inspectific Com Bugurag  No - Please provide details  Yes  Yes - Minimal logging  Yes - Other - Please provide details	Principles:  Our privacy policy is detailed out here: https://www.noredink.  Our 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 when the provide into the provide into the provide into the privacy of the pri
DSE13  DSE14  DSE14  SECTION 4 - LOGGING INFOR  LOG1  LOG2  LOG3  LOG4  LOG5  LOG6  LOG7  SECTION 5 - ACCESS AND AL  ACC1  ACC2  ACC3  ACC4	Data Privacy and Access  Data Privacy and Access  MATION Logging Access and Authentication Access and Authentication Access and Actherication Access and Actherication Access and Actherication Access and Authentication	product, is this functionality turned OFF by default?  Do you colled not yolds that customistics the minimum possible requirement necessary to operate the service or product, and fully supports the principle of data minimisation under the Australian Privacy Program of the principle of data minimisation under the Australian Privacy Program of the privacy of the service, analysis of the service, marketing and advertising disabled, links to unnecessary services disabled, geolocitation and other tracking disabled, links to unnecessary services disabled geolocitation and other tracking disabled, links to unnecessary services disabled, geolocitation and other tracking disabled, links to unnecessary services disabled, geolocitation and other tracking disabled, links to unnecessary services disabled, geolocitation and other tracking disabled, links to unnecessary services disabled, geolocitation and other tracking disabled, links to unnecessary services disabled, geolocitation and other tracking disabled, links to unnecessary services disabled, geolocitation and the activities performed?  Who has access to these logs?  Do you maintain security incident and event logs?  How long are these security logs retained?  Who has access to these security logs?  Do you usilistie as SIEM or other monitoring and alerting solution to triage and manage security events and incidents?  ORMATION  ORMATION  Does the solution provide unique usernames for all users?  How do you validate that the user is a legitimate user who should be granted access to the solution, and not an imposter?  How do you validate that the user is a legitimate user who should be granted access to the solution, and not an imposter?	MorPanel con Customer Jo Inspectific Com Bugurag  No - Please provide details  Yes  - Minimal logging  Yes - Minimal logging  Yes - Minimal logging  Yes - Minimal logging  Yes - Minimal logging  Yes - Minimal logging  Yes - Minimal logging (some elements of the solution)  Logs retained for 90+ days  3rd Party and internal administrative staff only  Yes - Other - Please provide details  Other - Please provide details  Other - Please provide details  No validation takes place  Other - Pease provide details	Principles:  Our privacy policy is detailed out here: https://www.noredink.  Our privacy policy is detailed out here: https://www.noredink.  comprivacy. 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 of the provide interview.  We use AWS CloudTrail, which gives logs about user access and infrastructure changes.  We have logs from our application servers, database servers, and load  We use AWS CloudTrail and CloudChecdr to help monitor system activity and support triage of security events and incidents. We don't currently have an elering solution in place.  Users can authenticate using a username and password, or an email and password, or use a Single-Sign-On solution. Google SSO or Cleve SSO.  User accounts are managed by the user, but teachers can also manage the accounts of their students.
DSE13  DSE14  SECTION 4 - LOGGING INFOR  LOG2  LOG3  LOG4  LOG5  LOG6  LOG7  SECTION 5 - ACCESS AND AL  ACC1  ACC2  ACC3  ACC4  ACC5	Data Privacy and Access  Data Privacy and Access  RMATION Logging Logging Logging Logging Logging Logging Logging Logging Access and Authentication	product, is this functionality turned OFF by default?  Do you rolled not yolds that cursuithus the minimum possible requirement necessary to operate the service or product, and fully supports the principle of data minimisation under the Australian Privacy Program of the product or service utilize features that ensure Privacy by Design's such as enforcing high privacy estimpts by detail (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, links to unnecessary services disabled, geolocation and other tracking disabled, links to unnecessary services disabled, geolocation and other tracking disabled, links to unnecessary services disabled, geolocation and other tracking of employee access to systems and data, and the activities performed?  Who has access to these logs?  Do you maintain security incident and event logs?  How long are these security logs retained?  Who has access to these security logs?  Do you uslike a SIEM or other monitoring and alerting solution to triage and manage security events and incidents?  ORMATION  Does the solution provide unique usernames for all users?  How do you validate that the user is a legitimate user who should be granted access to the solution on an imposter?  How are user accounts managed?  How are user credentials secured within the solution?  Does the solution support role based access?	MorPanel con Customer Jo Inspectific Com Buguriag  No - Please provide details  Yes - Minimal logging  Yes - Minimal logging  Logs retained for 90+ days  2rd Party and internal administrative staff only  Yes - Minimal logging (some elements of the solution)  Logs retained for 90+ days  3rd Party and internal administrative staff only  Yes - Other - Please provide details  Other - Please provide details  Other - Please provide details  For - Please provide details  Cother - Please provide details  Cother - Please provide details  Role based access (administrator, staff and student accounts)	Principles:  Our privacy policy is detailed out here: https://www.noredink.  Our privacy policy is detailed out here: https://www.noredink.  comprivacy. 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 of the provide interview.  We use AWS CloudTrail, which gives logs about user access and infrastructure changes.  We have logs from our application servers, database servers, and load  We use AWS CloudTrail and CloudChecdr to help monitor system activity and support triage of security events and incidents. We don't currently have an elering solution in place.  Users can authenticate using a username and password, or an email and password, or use a Single-Sign-On solution. Google SSO or Cleve SSO.  User accounts are managed by the user, but teachers can also manage the accounts of their students.
DSE13  DSE14  DSE14  SECTION 4 - LOGGING INFOR  LOG1  LOG2  LOG3  LOG4  LOG5  LOG6  LOG6  LOG7  SECTION 5 - ACCESS AND AL  ACC1  ACC2  ACC3  ACC4  ACC5  ACC6	Data Privacy and Access  Data Privacy and Access  MATION Logging Logging Logging Logging Logging Logging Logging Logging Logging Access and Authentication	product, is this functionality turned OFF by default?  Do you rolled not yield that cursitives the minimum possible requirement necessary to operate the service or product, and fully supports the principle of data minimisation under the Australian Privacy Program of the product or service utilize features that ensure Privacy by Design's such as errorioning high privacy estimpts by detail (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, links to unnecessary services disabled, service, marketing and advertising disabled, links to unnecessary services disabled, geolocation and other tracking disabled, links to unnecessary services disabled, services, marketing and advertising disabled, links to unnecessary services disabled, services, marketing and advertising disabled, links to unnecessary services disabled, services, marketing and advertising of employee access to systems and data, and the activities performed?  Who has access to these logs?  Do you maintain security incident and event logs?  Who has access to these security logs?  Who has access to these security logs?  Who has access to these security logs?  ORMATION  How does a user authenticate to the solution?  Does the solution provide unique usernames for all users?  How do you validate that the user is a legitimate user who should be granted access to the solution and on a imposter?  How are user accounts managed?  How are user accounts managed?	MorPanel con Customer Jo Inspectific Com Bugurag  No - Please provide details  Yes - Minimal logging  Yes - Minimal logging  Logs retained for 90+ days  2rd Party and internal administrative staff only  Yes - Minimal logging (some elements of the solution)  Logs retained for 90+ days  3rd Party and internal administrative staff only  Yes - Other - Please provide details  Other - Please provide details  Other - Please provide details  For - Please provide details  Cother - Please provide details  For - Please provide details  Encryption - Please provide details  Encryption - Please provide details  Encryption - Please provide details	Principles:  Our privacy policy is detailed out here: https://www.noredink.  Our privacy policy is detailed out here: https://www.noredink.  comprivacy. 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 of the provide interview.  We use AWS CloudTrail, which gives logs about user access and infrastructure changes.  We have logs from our application servers, database servers, and load  We use AWS CloudTrail and CloudChecdr to help monitor system activity and support triage of security events and incidents. We don't currently have an elering solution in place.  Users can authenticate using a username and password, or an email and password, or use a Single-Sign-On solution. Google SSO or Cleve SSO.  User accounts are managed by the user, but teachers can also manage the accounts of their students.

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 INFOR	RMATION						
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 Nofeelink al Eicense to translate, modify (for technical purposes, for example making sure the content is viewable on an iPhone as well as a compute) and reproduce such user submissions, in each case to enable us to operate the Services. This is a license only—ownership in user submissions in oral fetted.				
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 NoRedlink by submitting a written request via a Privacy Request Form (https://preferences.noredlink.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					
<b>SECTION 8 - EVIDENCE ATTA</b>	CHED							
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 permiss facilitate the developmen	sion for the responses above to be shared with other education jurisdictions to tt of a national standard						
Name Position								
			•					
Signature:	(electronic)	Date						
Forward this completed form and relevant evidence to the assessment team via email to niget hardy@kineticit.com.au								