ReadCloud Risk Review

Version: Paid (mobile version)

Overall risk level:	Medium *The overall risk level is the level of risk which remains after all treatments have been applied.*	**Review date:**	24/06/2019
Data hosting:	Onshore (in Australia)	**URL:** **Mobile App:**	https://www.readcloud.com/ ReadCloud (Windows, iOS, MacOS)
Purpose of use:	ReadCloud is a social eReader platform which lets students and teachers share annotations, videos and weblinks directly inside their eBooks. ReadCloud sources content from multiple publishers so all digital content is in one platform.		
Current availability and principal responsibility:	Unblocked for staff and students Although this service is unblocked on the department's network, it is recommended that principals read and accept the risks and risk treatments outlined in this review prior to using this service in their school. Principals accept full responsibility for the use of the service, including any associated risks, terms and conditions and legislative compliance (including responsibility for information involved in security breaches). Principals should also ensure users are aware of the risks and risk treatments. Principals can direct their MIS administrator to block this website at their school. Instructions on how to block a website at the school level can be viewed at *MIS Filtering: How to create a Block URL Filter package (KBA0020640).*	**Category**:	Education & Technology
Additional information:	• **This review encompasses the ReadCloud mobile application (Windows, iOS, MacOS)** • This service stores information onshore (i.e., within Australia), but it is outside the Department's network. This information is not protected by departmental policies or procedures.		

	• Teachers create student accounts for this service. • Teachers and students are organised into virtual classrooms (clouds) and the appropriate content is provisioned into these clouds. • Students only download ebooks they are assigned by the teacher from the ebooks licenced to the school. • School settings can be applied to allow or restrict third party content e.g. YouTube. • Students can upload their own content to read in this platform. They cannot share this content with others. • This service has unauthenticated access applied to ensure the application can connect to the school's network. This removes the ability to report on specific users or user groups accessing this application.

Personal information entered during account creation:	☒ Name ☐ Date of Birth ☒ Gender	☐ Profile photo ☐ Address ☐ Phone number	**Parent/guardian consent:** **Information security classification:**	Parent/Guardian consent is required as personal information is disclosed to register an account – see consent form Consent Form X-in-confidence
	Schools are encouraged to keep a centralised register of the third party websites, web applications, and mobile applications with whom students' personal information is shared. See MIS – Online service risk reviews: Guidelines for using online services (KBA0027172) for more information.			
Terms of Use:	https://www.readcloud.com/terms		**Privacy Policy:**	https://www.readcloud.com/privacy

Risks and Risk Treatments

After conducting a comprehensive review, the department has identified that the following risks apply to this service. The risk treatments listed are designed to reduce risk exposure. Users must adhere to all stated risk treatments when using this service. To learn how risks are identified and treated, please view *MIS – Online service risk reviews: Risk levels explained (KBA0027040)*

Risk	Risk treatment	Risk level

Account registration is required to access this service. In doing so, information is disclosed to a third party service not managed by or contracted to the department. This increases exposure to risks associated with legislative compliance (e.g., information privacy, information security, child/student safety etc.). When creating an account using the standard account creation process, the following mandatory information is disclosed: • **Email address** • **First name (personal information)** • **Surname (personal information)** • **Phone number (personal information)**	This service allows an administrator or teacher to register accounts on behalf of students using education setting/options. Where possible, teachers should register accounts for students. When registering an account using the education options/settings available within the service, the information below is disclosed. • **Email address** • **First name (personal information)** • **Surname (personal information)** • **Age** • **School name** • **Gender (personal information)** • **Year level** In accordance with the Information Privacy Principles set out under the Information Privacy Act 2009 (Qld), consent is required from the individual, or in the case of a minor, consent is required from the parent/carer to use and disclose personal information**. If personal information is disclosed** and stored within the service, use the Consent Form to obtain parent/carer consent. If no personal information is disclosed, parental consent is not required. Ensure only mandatory fields are completed when registering accounts, and use departmental details in place of users' personal details wherever possible (e.g., departmental email address instead of personal email address, departmental MIS ID as a username). Do not use departmental passwords when creating an account.	**Medium**
When registering an account for this service, users may unwittingly subscribe to the service's mailing list. This may result is unwanted communication (e.g., promotional materials, emails etc.)	Check user account/profile settings to ensure users are not subscribed to the service's mailing list (e.g. newsletter, emails, updates).	**Low**

When registering an account for this service, users are required to enter accurate and complete information. Users are unable to use de-identified information (e.g. pseudonyms or avatars).	Departmental details should be used in place of students' personal details, where possible (e.g., departmental email address instead of personal email address, departmental MIS ID as a username, school address instead of home address, school phone number instead of home/mobile phone number).	**Medium**
This service imposes an age restriction on its users.	Use of this service is restricted to users aged 18 and over however, users under the age of 18 can use the service with parental consent.	**Low**
This service may store information without encryption. Encryption ensures that only authorised users can access your stored information. Information that is not encrypted is not considered to be secure.	No treatment is available for this risk.	**Medium**
This service supports multi-tenancy for enterprise customers however, it does not employ adequate encryption and/or security controls to protect stored data. Encryption ensures that only authorised users can access your stored information.	No treatment is available for this risk.	**Medium**
This service allows users to engage in communications with other account holders through commenting. These communications have some moderation and/or breach reporting or removal features. Users may be exposed to online predators and or inappropriate content or comments.	Functionality exists to allow an administrator to disable or restrict the permissions for commenting within this service. Use this functionality to restrict communication to known users only (e.g., peers).	**Low**
This service allows users to create and store and/or upload data (e.g., work files, academic results, medical information, images, video and or audio). Stored or uploaded content may include personal information, departmental data, and/or intellectual property/copyright materials.	Users must not upload any material (e.g., written, audio, video etc.) that they do not own or have not created, or any material that infringes Intellectual Property rights such as copyright. Users must not upload or create content that contains personal (e.g., information that could be used to identify the user, including photos) or sensitive departmental information. Sensitive departmental information should only be stored in departmental systems (e.g., OneSchool). Information from OneSchool should not be uploaded to this service.	**Medium**

This services allows users to download files. Downloading files from the internet presents a risk to the department's network as this increases potential exposure to malicious content or malware. Uploading and/or downloading large files may impact your school's bandwidth utilisation which may affect internet speeds.	Ensure users are aware of the risks of downloading unknown files for both their device and the department's network. For more information, visit the iSecurity ebsite (https://isecurity.eq.edu.au). Refrain from downloading large files during school hours.	**Medium**
Payment is required to access this version of the service.	The department does not endorse the use of any product or supplier. Before making any decision to purchase, ensure you have assessed, at a minimum, the product's educational benefits, value for money, and risks. Ensure payment is made through a secure method. The following options represent secure payment methods: • those facilitated by PayPal, BPAY, Purchase Orders, Invoices, Visa's Verified by Visa and MasterCard's SecureCode. • payment pages with "https" at the beginning of the url	**Low**
This service may not offer integrated data loss prevention capability. This increases the risk of unauthorised access to sensitive data while it is in use, in transit, and at-rest.	No treatment is available for this risk.	**Medium**
This service may not perform routine penetration testing. Penetration testing proactively seeks to evaluate the security of IT infrastructure by safely trying to exploit vulnerabilities.	No treatment is available for this risk.	**Medium**
This service may not log administrator activities. In the event that the service provider's administrators perform actions that impact end users, there may be no ability to review these activities.	No treatment is available for this risk.	**Medium**
This service may not log end user activities. This means that there may be no ability to review actions performed by end users (e.g., in the event that chat logs were requested for a cyber-safety investigation).	No treatment is available for this risk.	**Medium**

This service may not log access to databases. This means that there may be no ability to review actions performed by users and/or administrators when accessing databases (e.g., in the event that data is edited or removed).	No treatment is available for this risk.	**Medium**
This service uses user activity tools. This may include cookies, beacons, tags, google analytics, and/or scripts. These tools monitor a user's online behaviour to provide feedback to the service or target advertising to the user.	As this service uses activity and tracking tools we recommend you: • Clear your cookies and cache on a regular basis. • Be aware that your activities may be tracked and you may receive targeted advertising from this service or others.	**Low**
In the event that legal proceedings occur, these may fall outside of Australia's legal jurisdiction. This means that Australian legal protections and legislation may not apply, and/or disputes between the service provider and users may occur outside of Australia.	No treatment is available for this risk.	**Low**
The service provider does not specify the statute of limitations that applies in the event of legal proceedings. This means the maximum time that parties have to initiate legal proceedings from the date of an alleged offense may not be governed by Australian legislation.	No treatment is available for this risk.	**Medium**
The service's Secure Sockets Layer (SSL) Certificate is due to expire in 12 months or less. If the SSL certificate was to expire, data transferred between the web server and the web browser would no longer be encrypted. Encryption seeks to ensure that only authorised users can access the information. Information that is not encrypted is not considered to be secure.	No treatment is available for this risk.	**Medium**

The strength of the signature algorithm used by the Service's Secure Sockets Layers (SSL) Certificate is inadequate. The strength of the algorithm used in signing a digital certificate is a critical element of the security of the certificate. Weaknesses in algorithms can lead to situations in which fraudulent certificates can be created or obtained.	No treatment is available for this risk.	**Medium**

Please note: *While the information in this review is considered true and correct at the date of publication, subsequent changes may impact its accuracy. Please log a job through this Service Centre online form to advise if any content within this review requires an update. Adherence to the risk treatments outlined in this document does not guarantee information security and user safety while using the service*.

Internal purposes only: *Risk reviews are completed for department employees and intended for internal use only. They are not intended for external distribution. If website owners and vendors are seeking feedback on their review, they are welcome to submit a right to information request.*

Legislation, Procedures and Guidelines

Websites, web applications, and mobile applications are assessed and reviewed to inform departmental employees about the security, information privacy and safety implications of using third party services on the department's network. The risks and risk treatments outlined in this review are identified in compliance with the state legislation and standards and departmental procedures and frameworks. For more information, please see *MIS – Online service risk reviews: Frequently asked questions (FAQ) about Risk Reviews (KBA0027738).*