Australian
National
University

Privacy Impact Assessment

For

Proctorio

Contents

1. Introduction

The end of semester in-person invigilated examinations held in June (and November) each year consist of approximately 400 exams, with 2000 students per sitting (2 per day) – a total of 45,000 individual exam sittings. If exams cannot be held students may not be able to graduate from their degree or progress into semester 2 subjects. To mitigate against this, we are considering options for replacing in-person invigilated exams with remote exams.

1.1 Project objective and Scope

In recent years there have been significant advances in remote proctoring (invigilation) products, which incorporate similar processes of recording the student as they take the exam, recording keystrokes etc from their computer, and using a combination of AI (Artificial Intelligence) and human observation to identify possible cheating behaviours.

We are seeking to integrate a remote proctoring (invigilation) service with Wattle to provide assurance of student identity and academic integrity at scale throughout timed examinations using one of these Wattle tools.

Timing is tight. It usually takes many months to work through the details of choosing, licensing, and integrating new software with Wattle. Minor upgrades to Wattle occur on a monthly schedule set by our provider (Blackboard) and both our ITS staff and Blackboard need to step through many checks to ensure that the integration will be successful and will not break other parts of Wattle. The earliest Wattle upgrade where we could possibly get a remote proctoring service integrated with Wattle added is the **29th of April**. Having undertaken a market scan Proctorio[1] appears to best meet the requirements for remote invigilation of Moodle-based assessments in Wattle.

1.2 Timelines

The preferred timescale is included below;

Planned Start Date:		**Planned End Date:**	

1.3 List of stakeholders

Below is the list of key stakeholders identified for this project.

- Examinations office
- Academics – Colleges as represented buy ADEs, individual academics with particular assessment requirements
- ITS: Contracts management; IT Security; Teaching and Learning Technology team; Learning Systems Support Group
- CISO
- Privacy officer
- ASQO – policy support
- College Educational Support Teams, CL Educational Designers – support academics to implement online assessment
- Student representatives: ANUSA, PASRA
- Access and Inclusion

[1] https://proctorio.com/platform

- Executive and governance oversight: DVCA, PVCE, CMT; TLDC, AQAC, Academic Board
- RSCS - have particular technical requirements that don't align with Wattle

1.4 Key privacy elements

1.4.1 Type of information that will be collected in the new system

Proctorio collects personal information only in the form of a video of the student during their exam. Proctorio supports single sign-on to verify user. The User credentials are an authentication factor done by the LMS and what the LTI points to when recording, no data is stored during this process.

The single sign-on and settings are within Moodle. If a student has access to the test or course within Moodle, then Proctorio will add in the added layer of authentication to initiate for the attempt.

Proctorio can capture the user's video during the exam period which will be stored in Microsoft Azure's Data Centre within Australian geographic region.

1.4.2 How the new system will address the security and information quality?

1. The database will be hosted in the cloud server environment of the vendor. The data security and privacy details around this environment have been provided by the vendor.
2. The CISO has advised that the system meets the University's cybersecurity requirements.
3. All access requests will follow the standard system access protocols of the University and all users will need to read and agree to abide by the conditions detailed in the below documents,
    - Acceptable Use of Information Technology: https://policies.anu.edu.au/ppl/document/ANUP_001222
    - Account Management and Access: https://policies.anu.edu.au/ppl/document/ANUP_000709
    - Privacy Policy: https://policies.anu.edu.au/ppl/document/ANUP_010007
    - Code of Conduct https://policies.anu.edu.au/ppl/document/ANUP_000388
    - Information Technology Security https://policies.anu.edu.au/ppl/document/ANUP_000421
    - ANU Enterprise Agreement https://services.anu.edu.au/human-resources/enterprise-agreement
4. A dedicated system support team will be provided by the vendor.
5. System Administrative permissions will be given to Wattle BSG team members. They will be coordinating with relevant course directors to enable the services wherever necessary.

1.4.3 How the information will be used and disclosed?

The activity for which the data captured by Proctorio will be used to:

- allow the test or exam taker to complete the activity.

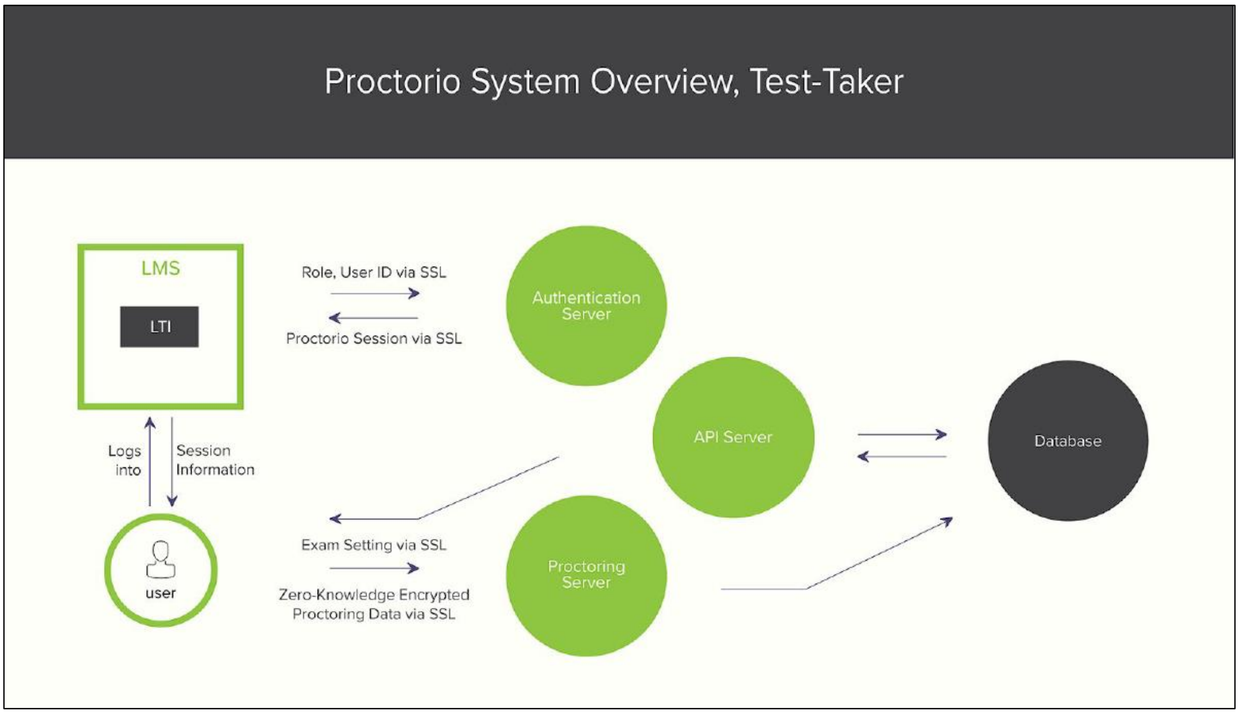
- Manage exam parameters, computer requirements, account information, faculty controls, and Gradebook settings
- Information stored in Proctorio can only be viewed by
  - The test taker
  - the education staff who require access to ensure appropriate individuals are taking the test properly

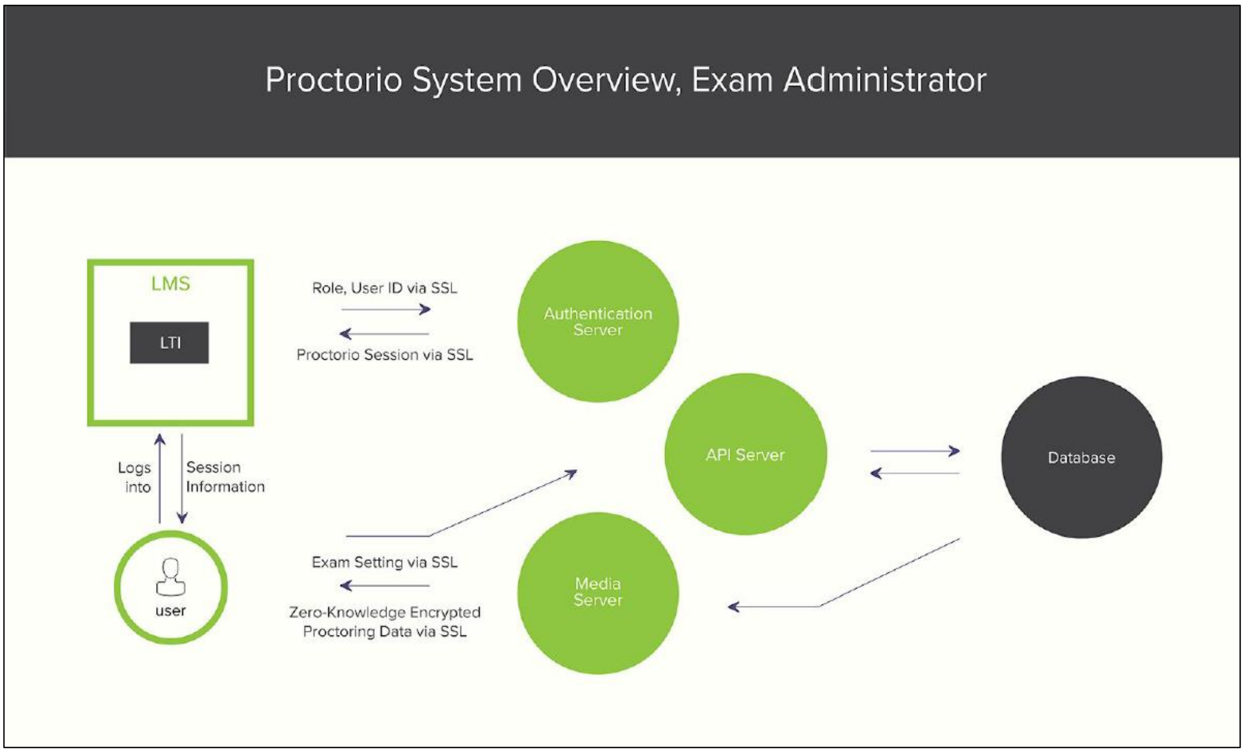
Staff in the school and the Registrar's office enable the recording of the results of the assessment.

1.5 Information flows

Media Server stores the personal information in the form of video. This video (data) is accessible via encrypted proctoring Data via SSL. Proctorio maintains zero-knowledge encryption where they will have no access to any personal data.

The authentication and data flows can be simplified to these two diagrams based on role:





Proctorio System Overview, Exam Administrator

1.6 Privacy issues and actions

The key issues in respect of privacy are:

- Ensuring the information that is in the system is correctly managed – so that access is available only to those who require access to enable academic progress for the students
- Ensuring that those ANU staff with access are appropriately trained including in privacy and confidentiality of organisational information.
- Ensuring that information is not available to those who should not have access
- Ensuring the information is not available to third parties
- Ensuring that information can be corrected it if is incorrect
- The system will contain a log file of all access so that there is an audit trail

Items for action are:

- **Ensuring only the required personal information is provided for use of Proctorio.**
  - No personal information will be communicated to Proctorio**.**
- **How it will be ensured that the information that is in the system is managed consistently with the privacy policy?**
  - Access will not be available to any individuals who are not ANU staff members with a need to access the information in order for the student's academic progress (primary purpose of personal data being held by ANU)
  - ANU Staff will be trained in privacy and confidentiality. All staff with access are employed by ANU and required to comply with the ANU Policy and Code of Conduct.

  - An audit trail of access occurs through system logs
  - ANU staff behaviour is managed through the code of conduct and employment conditions requiring compliance with policies and legislation.

- **What privacy controls are in place for access to information and its use?**
  - Only ANU staff will have access to Proctorio. System access is only granted to ANU employees.
    - Every new user will be trained. They are required to comply with policies and legislation under their employment conditions. Acceptable Use of Information Technology: https://policies.anu.edu.au/ppl/document/ANUP_001222
    - Account Management and Access: https://policies.anu.edu.au/ppl/document/ANUP_000709
    - Privacy Policy: https://policies.anu.edu.au/ppl/document/ANUP_010007
    - Code of Conduct: https://policies.anu.edu.au/ppl/document/ANUP_000388
    - Information Technology Security: https://policies.anu.edu.au/ppl/document/ANUP_000421
    - ANU Enterprise Agreement: https://services.anu.edu.au/human-resources/enterprise-agreement
  - All staff given access will be required to complete the Pulse Privacy module before they are granted access to the system. Supervisor of the new user will have to authorise this access.
  - Training materials and user guides will include guidelines for handling personal and sensitive information. Training material will be revised and updated on a regular basis to reflect any changes in the system processes or privacy laws.
  - Regular refresher training will be available to all users and users will be reminded of their privacy and user of data obligations on an ongoing basis through regular items in user communications, including newsletters and information sessions.
  - Access will be removed promptly when staff leave the area.

- **What system controls will be in place?**
  - The security of the system has been assessed and approved by the Chief Information Security Officer on 8 April 2020
  - Users will be assigned to system roles with access to records and functionality as is appropriate to their position.
  - The system has a log which records details of all user interactions including user details, time stamps and data which was modified/entered/viewed.

- **Correction of personal data**
  - Not relevant as no personal information is sent to or held in the system..

- **What mechanisms/controls will be in place to ensure that the information is used only for the primary purpose for which it is collected?**
  - All staff with access will be trained and required to ensure access is consistent with the primary purpose for which the personal information is provided i.e. academic progress.
  - No third parties will have access to or be provided with the personal information.

2. Conclusion

This Privacy Impact Assessment (PIA) document has been created based on the PIA guidelines set out by the OAIC (Office of the Australian Information Commissioner).

The project team will review and update this PIA document when any changes in the Procotorio system make this necessary.

The project team will also work closely with the ANU privacy officer for necessary guidance around the privacy compliance requirements throughout the implementation.

Approved

Roxanne Missingham
Privacy Officer

9 April 2020