**Cloud Services Hosted - Data Classification**

To assess the Security Risk to UTAS in the event that the service is compromised we need to evaluate the data classification and data flows hosted in the application provided as a Cloud Service.

Does the application contain Personal Information (PI)?

* The application does **not** **store** any personal information.
* The application **retrieves** personal information for display as outlined in the “Discord Bot Questions” document.
* The application **stores** an MyLO OAuth token and refresh token for a student, which can be used to retrieve personal information and the Sensitive PI (pronouns) if the token is accessed.
  + This token is stored in an **encrypted** format on a secure database.
  + This token is **never** transferred to the Discord user client, as it is only used by the server to make authenticated requests.
  + This token expires every 20 hours and must be refreshed.
  + More information about the storage of this token is explained in the “Discord Bot Questions” document.
* **No other** Personal Information from MyLO is stored by the application.

Does the application contain data that is classified Sensitive PI?

* The application can **retrieve** the chosen pronouns of the currently authenticated student if the student has this information stored on MyLO.
  + This information is **not** **stored** by the application.
  + This information is **not** **collected** by the application.
* **No other** Sensitive PI from MyLO is retrieved or stored by the application.

Does the application contain Intellectual Property (IP)?

* The application is being developed by a University Staff Member on University time, and is itself **IP of the University**.
* The content of a unit MyLO page is IP of the University and may be **retrieved** by the application.
  + This content is **not stored** by the application.
  + Only content that the authenticated student or unit coordinator could **normally access** via the MyLO website can be retrieved.
  + In most cases, retrieval only obtains a **link** to the MyLO website content item.
* **No other** IP is retrieved or stored by the application.

Is the data encrypted at Rest (By the application)?

* **Yes**, the OAuth token is encrypted when stored in the secure database

Is the data encrypted in transit?

* **Yes**, all MyLO API requests use HTTPS

Is the data encrypted at Rest (Client side)?

* **No –** no personal information is stored client-side.
  + OAuth token is not sent to client
  + All retrieved personal information is shown in the Discord client in an “ephemeral” message which is visible on the user’s screen until they close Discord or 15 minutes have elapsed. This information is **not** stored on Discord servers, and **not** stored on the user’s hard drive.

Please provide a complete list of all Data Attributes stored by the application.

* Only the authenticated user’s OAuth token is **stored**.
* **Retrieved** information (as outlined in “Discord Bot Questions” document in more detail):
  + Student-level information:
    - Student ID
    - First Name
    - Last Name
    - Pronouns
    - Enrolled units past and present
    - Grades (Assessment item, score, feedback)
    - Assessment completion
  + Unit Coordinator-accessible information about students
    - Campus and Tutorial Allocations (accessible to unit coordinator via queries to “group enrolment”, where groups are automatically populated for students).
    - Email
    - Role (student, tutor)
    - Last access date
    - Current MyLO online status (true/false)
  + Unit info:
    - Assessment items and due dates
    - Content items and meta data
    - MyLO Unit Identifier

Definitions Detailed below are taken from the Australian Government – Office of the Australia Information Commissioner (OAIC) web site:

**How does the Privacy Act define ‘personal information’?**

The Privacy Act defines ‘personal information’ as:

**‘Information or an opinion about an identified individual, or an individual who is reasonably identifiable:**

1. **whether the information or opinion is true or not; and**
2. **whether the information or opinion is recorded in a material form or not.’**

The definition is technologically neutral to ensure sufficient flexibility to encompass changes in information-handling practices over time. It is also consistent with international standards and precedents.[**[2]**](https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information#ftn2)

**The Privacy Act: Some Important Definitions**

**Sensitive information**

6.88 ‘Sensitive information’is a sub-set of personal information and is given a higher level of protection under the NPPs. The IPPs do not refer to sensitive information and agencies are required to handle all information, including sensitive information, in accordance with the IPPs. The principles recommended for handling sensitive information, and their extension to agencies, are discussed further in Chapter 22.

6.89 ‘Sensitive information’ is defined in the *Privacy Act*to mean information or an opinion about an individual’s:

* racial or ethnic origin;
* political opinions;
* membership of a political association;
* religious beliefs or affiliations;
* philosophical beliefs;
* membership of a professional or trade association;
* membership of a trade union;
* sexual preferences or practices; or
* criminal record.

6.90 ‘Sensitive information’ also includes health information[[98]](https://www.alrc.gov.au/publications/6.%20The%20Privacy%20Act%3A%20Some%20Important%20Definitions/sensitive-information" \l "_ftn98) and genetic information about an individual that is not otherwise health information.[[99]](https://www.alrc.gov.au/publications/6.%20The%20Privacy%20Act%3A%20Some%20Important%20Definitions/sensitive-information" \l "_ftn99)

6.91 ‘Sensitive information’ is subject to a higher level of privacy protection than other ‘personal information’ handled by organisations in the following ways:

* ‘sensitive information’ may only be collected with consent, except in specified circumstances. Consent is generally not required to collect ‘personal information’ that is not ‘sensitive information’;[[100]](https://www.alrc.gov.au/publications/6.%20The%20Privacy%20Act%3A%20Some%20Important%20Definitions/sensitive-information" \l "_ftn100)
* ‘sensitive information’ must not be used or disclosed for a secondary purpose unless the secondary purpose is directly related to the primary purpose of collection and within the reasonable expectations of the individual;[[101]](https://www.alrc.gov.au/publications/6.%20The%20Privacy%20Act%3A%20Some%20Important%20Definitions/sensitive-information" \l "_ftn101)
* ‘sensitive information’ cannot be used for the secondary purpose of direct marketing;[[102]](https://www.alrc.gov.au/publications/6.%20The%20Privacy%20Act%3A%20Some%20Important%20Definitions/sensitive-information" \l "_ftn102) and
* ‘sensitive information’ cannot be shared by ‘related bodies corporate’ in the same way that they may share other ‘personal information’.[[103]](https://www.alrc.gov.au/publications/6.%20The%20Privacy%20Act%3A%20Some%20Important%20Definitions/sensitive-information" \l "_ftn103)