



SIA Corporate Services Privacy Impact Statement

Version 1.0

Terms of Reference	1
Privacy Impact Assessment	1
Project Summary	1
Scope of Impact Assessment	2
System Information Flow	2
Privacy Impact and Compliance Analysis	4
Privacy Risks	4
Privacy Impact Analysis	4
Australian Privacy Principal Relations	5
Privacy Management assessing the risks	8
Summary of risks	8
Response to risks	8
Conclusion	9
Relevant Legislation, Policies and Guidelines	10
Appendices	11
Appendix A	11

Terms of Reference

Users	Sport Integrity Australia Employees, excluding casual staff (Chaperones)
PI	Personal Information which can include sensitive Personal Information
The app(s)	The SIA Corporate Services Application
IPO Report	Information of Position Occupant Report

Privacy Impact Assessment

Project Summary

The SIA Corporate Services (the app) is Microsoft PowerApps application that unifies internal workflows by integrating processes from Finance, Human Resources, ICT Property and Security, and Travel into a single, centralised location. Currently, these processes operate independently and inconsistently, and fragment access to data.

By consolidating these processes into one central user-friendly interface, the app provides a more efficient and consistent experience for staff.

The application includes the following workflows:

- Conflict of interest
- International travel approval flows
- Finance spending proposals
- Outside employment
- Incident reporting
- IT service desk

The app is expected to include additional workflows such as Gift and Benefit declarations, flexible working arrangement applications, and more.

The current build of the project utilises SharePoint Lists and its inbuilt security features to store and record information. In combination with Microsoft Power Automate, SharePoint Lists provide row level security to manage access to records.

Whilst the current solution satisfies baseline privacy requirements, additional funding for the implementation of PowerApps Premium would further strengthen security controls to Personal Information (PI) and provide a scalable relational database.

The app is developed and maintained by the ICT Team and enables key stakeholders within the agency to automate their workflows.

Scope of Impact Assessment

This PIA considers the stakeholders, information, and components and processes relevant to the app.

Stakeholders

SIA and SIA staff who are required to complete governance disclosures and declarations. As a Federal Government Agency, these attestations are crucial in allowing SIA to maintain its integrity and compliance with the APS Code of Conduct.

Information

The app manages and stores the PI of staff which in some cases may be sensitive PI. This may include personal/contact details, identifiers such as AGS, health information, accessibility requirements, workplace incidents, and conflict information.

Components and Processes

The Microsoft Power Platform hosts the application and stores the information within SIAs Microsoft Tenancy. The app uses Power Apps and Power Automate to present, and manage information, and uses SharePoint to store information.

Whilst the app provides a medium for which to modify and store information. The use and disclosure of PI remains with the workflow owners; where applicable, workflow owners may apply their own Privacy Policies and practices in line with their requirements.

This PIA does not assess the impact and security of legacy and deprecated systems and does not extend to major future changes or system redesigns, which should be considered separately.

System Information Flow

Information which is submitted by users is handled and processed by Power Automate. Power Automate allows for access control to records to be automatically applied to relevant staff. Data stored in SharePoint can be accessed through the app and directly through SharePoint which determines access rights to records.

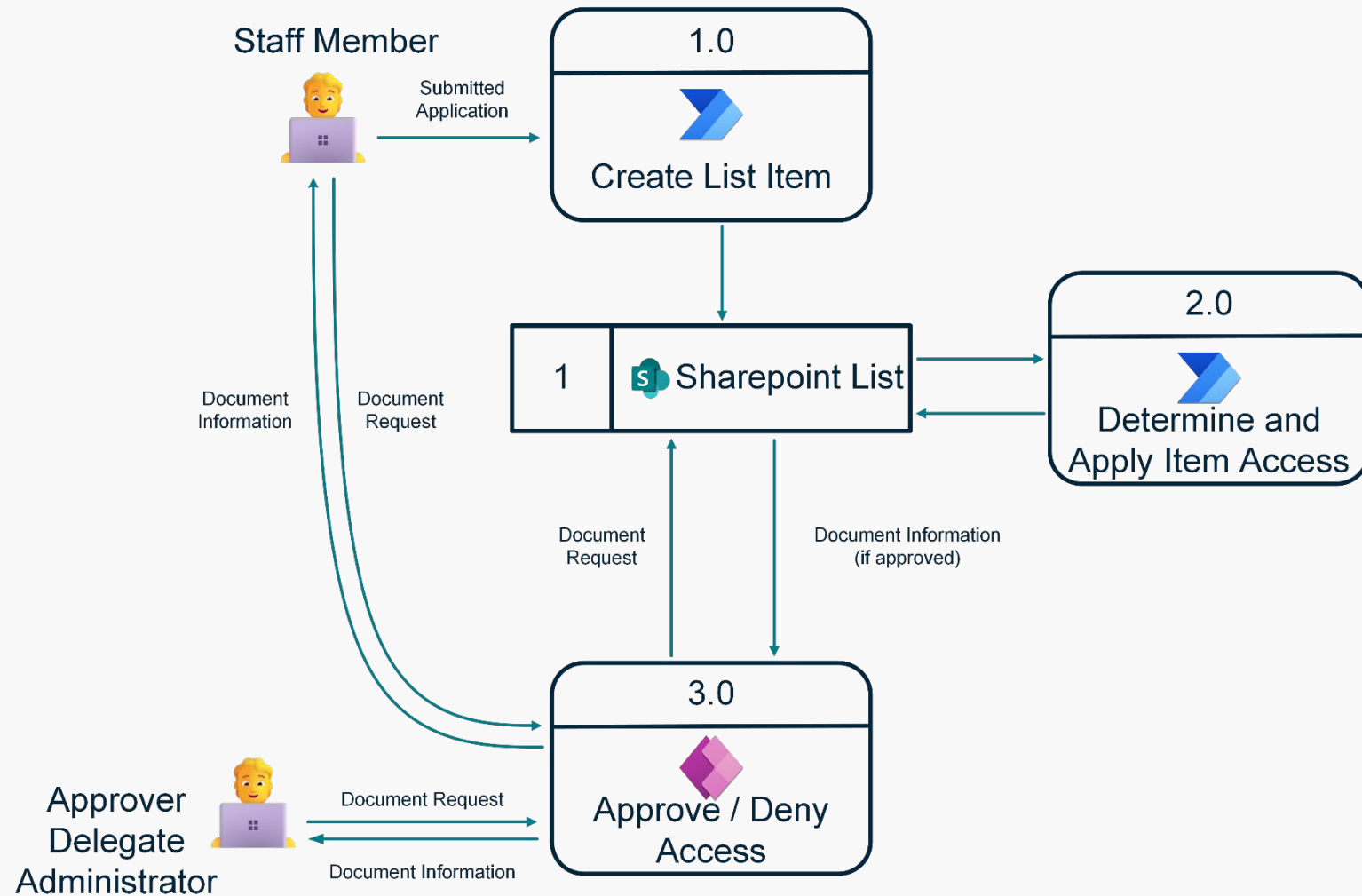


Figure 1.0 – High Level Data Flow Diagram of The App

Privacy Impact and Compliance Analysis

Privacy Risks

The following privacy risks have been identified:

Unauthorised Access to Personal Information

Unauthorised access to sensitive PI may occur in cases where misconfigured SharePoint access is applied. Delayed or incorrect IPO data may also lead to unauthorised access, as access to records is determined by position numbers obtained from the SAP IPO report.

Data Leakage through Integrations

Integrations such as Power Automate may in some cases fetch data automatically when information is created in SharePoint. This may result in an individual collecting data with automation which they should not be permitted to access.

Inability to audit log access

Microsoft Lists does not have the ability to collect logs on viewed information and viewed lists. This means that there is no detailed information which shows user access to specific lists and records.

Exposure

The exposure of information by staff to third parties is a potential risk. These third parties can include and are not limited to unauthorised staff, non-affiliated individuals/entities, and external platforms/digital services.

Privacy Impact Analysis

Whilst the apps' purpose is to provide a platform to allow staff to view and manage PI, the collection of this information is necessary due to SIAs requirement as an employer and Federal Government Agency. The method of collection differs to the current workflows; however, the use and disclosure of PI remains the same.

The app automates and unifies current corporate workflows and does not develop new uses and applications of PI.

As the use and disclosure of PI remains the same, the apps collection of PI aligns with stakeholder expectations and privacy values.

Australian Privacy Principal Relations

To ensure compliance with the APP the following steps have been taken:

APP 1

A privacy policy for users of the app has been written and will be made available to staff. (Please see appendix A.1 for the privacy policy).

This policy will be updated should new workflows, modifications to workflows, or major updates to the apps components and/or processes be developed. Contacts for staff to make inquiries and complaints is included should they be required.

APP 2

Not applicable as the applications purpose is to store information regarding staff and their employment.

APP 3

The collection of PI is required and is necessary for the purposes of the app.

The following PI is stored in SharePoint:

- Staff information
- Staff conflict details
- Conflict management plans
- Travel accessibility requirements
- Staff Outside employment details, employer and position details
- Workplace incident details, including staff involved and details of the incident.
- Flexible working arrangements including details and justification for arrangements.

Staff provide required personal information (required under the APS Code of Conduct) to SIA to satisfy the agencies functions, activities, and requirements as a Federal Government Agency.

Personal Information about an individual which is not provided by the individual is collected in cases where SIA is authorised and required as an employer to record certain attestations.

APP 4

There may be cases where an employee submits sensitive PI in relation to another employee such as in the case of workplace incidents. This information can be collected as outlined under APP 3 above.

Destruction or deidentification of this information may not be reasonable as under Work Health and Safety regulation, employees are required to report incidents such as physical and/or psychological hazards occurring within the workplace.

PI which does not satisfy APP 3 and meets APP 4.3, can be deleted by the ICT, Property and Security team, or by the workflow administrators.

APP 5

Information collected by workflow owners is subject to their information privacy policies, and as such, the processes and procedures relating to the notification of collection of PI is subject to the respective workflow privacy policies.

APP 6

The PI disclosed is used by the relevant teams and staff who own and are required to act in the specific workflows, and the information is subject to the respective privacy policies.

APP 7

Not applicable as PI disclosed is not used for marketing.

APP 8

Not applicable as PI is not disclosed overseas.

APP 9

The use of a government related identifier (AGS Number) may in some cases be required and is permitted under APP 9.24 (An organisation may use or disclose the government related identifier of an individual if the use or disclosure is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions (APP 9.2(a)).)

APP 10

Information entered into the app should adhere to APS Code of Conduct. Should information be inaccurate and require correction, users of the app can amend and update PI, alternatively, ICT can amend and correct information in cases where users are restricted from making changes to information.

APP 11

Reasonable steps are taken to protect PI; Microsoft access controls provide relevant parties (i.e. PI Creator, approvers, delegates and/or workflow administrators) with access to specific records. Version history is available allowing record changes to be recorded.

APP 12

Access to PI is available to staff to which the PI relates and can be determined by workflow privacy policies. Access may be adjusted due to Position Occupant changes.

APP 13

Information can be corrected and amended should this be required. Staff can contact HR and ICT to correct information should it be incorrect.

Privacy Management assessing the risks

SharePoint lists are configured to (by default) only permit the record creator to access the record. Access is then provided to relevant users by automations which determine access from IPO data. Delays in processing this data may allow previous position occupants to view data no longer relevant to them. Previous position occupants shall maintain visibility over records in which they have made governance actions. Additionally, users can be assigned roles by workflow administrators which permit record access and management; misconfigured or delayed access management may lead to unauthorised access to PI.

Record permissions for users apply to any automations created and owned by users. This mitigates the risk of data leakage through service integrations by only permitting a user to fetch information (through automations) which they would be permitted to view.

Finally, APS Code of Conduct prohibits the improper use, disclosure or handling of official information which includes PI.

Summary of risks

The occurrence of the identified risks occurring from the development and design of the application can be considered low as there are ongoing mitigations and access controls in place aiming to prevent unauthorised access; in addition to these mitigations, Law, Policy and Legislation prevent the misuse and disclosure of PI by the users of the app.

Response to risks

In the case of incorrect access, ICT will immediately, when notified, manually remove access and investigate if the access was granted due to incorrect data or due to an error in the logic of the flows providing viewing access. The result of investigations will inform and direct remediations to prevent and resolve privacy incidents or unintended disclosures of personal information.

In addition to the above, ICT may conduct access audits to ensure information from workflows is available only to relevant staff.

Conclusion

The SIA corporate services application is a centralised corporate governance system that unifies and automates multiple agency attestation workflows. Whilst technologies used may allow for unauthorised access to PI, policy, law, legislation, and mitigations are in place to prevent the misuse and unauthorised disclosure of PI. Future builds of the app that introduce new privacy risks should be subject to separate review.

Overall, the current processes and mitigations are sufficient in protecting the PI of SIA employees. To ensure the continuous protection of PI, ongoing monitoring and audits are recommended to ensure compliance with the apps privacy policy and requirements in handling personal information.

Relevant Legislation, Policies and Guidelines

APS Code of Conduct, Australian Public Service Commission, 2023

Australian Privacy Principles, Office of the Australian Information Commissioner, 2019

Privacy Act 1988 (Cth)

Public Service Act 1999 (Cth)

Appendices

Appendix A

Privacy Policy

The SIA Corporate Services Application (the application) collects and stores information relating to various corporate workflows. These workflows include and are not limited to, Conflict of Interest declarations, Workplace Incidents, Gift and Benefit Declarations and Notification of Outside Employment.

Personal Information submitted in these workflows is stored in SharePoint and shared with the respective workflow teams and any relevant approvers / delegates. Sensitive Personal Information which you mark as 'Private' will only be visible by you and to your selected HR representative.

SIA ICT Support may have privileged access to the databases that store your personal information. This access is provided solely for the purpose of maintaining and supporting the application, resolving technical issues, and ensuring the security and integrity of our services.

If you have any concerns, please contact itrequests@sportintegrity.gov.au or humanresources@sportintegrity.gov.au.