BENDIGO DISTRICT RSL

Privacy Impact Assessment

Facial Recognition Technology

Introduction

Bendigo District RSL Sub-Branch Inc. (**Bendigo RSL**) is considering a program for the introduction of Facial Recognition Technology **(FRT**) at its licensed gaming venue, Bendigo District RSL: 73-75 Havilah Road Bendigo Vic 3550 (**Premises**) (**the Program**).

This privacy impact assessment (**PIA**) is undertaken to analyse how the Program may impact on the information privacy of its members and guests (**Patrons**), as well as the wider community. The PIA will identify the kind of personal information captured by the Program, identify potential privacy risks, develop risk mitigation strategies and practices, and assess the suitability of the Program.

The purpose of the Program is to use FRT to help meet legal obligations under the *Gambling Regulation Act 2003* (**the GRA**) which requires venues to take steps to prevent banned or self-excluded patrons (**BSEPs**) from areas of the Premises.

The PIA is divided into five parts:

- Part 1 – Program background and details
- Part 2 – Privacy analysis
- Part 3 – Privacy risk assessment
- Part 4 – Assessment and conclusion
- Part 5 – Action items, Board approval and document information.

Part 1 – Program background and details

Program	Introduction of Facial Recognition Technology		
Organisation	Bendigo District RSL Sub-Branch Inc. (ABN 32 661 050 883)		
Program Manager	Martin Beekes	Email	office@bendigorsl.com.au
Privacy Officer	Dianne McCullagh	Email	office@bendigorsl.com.au
Date Completed	04/03/2026		

Description of the program and parties

Bendigo RSL is seeking to introduce FRT to help identify and prevent BSEPs from gaining access to the Premises.

Currently BSEPs are prevented access in reliance on manual cross-checking by staff of Patrons attending the Premises with images provided by BSEPs in connection with their exclusion. The Premises currently has more than 315 BSEPs at the Premises.

The Program is in response to prevailing industry concerns about ensuring that gaming premises can adequately prevent access to the Premises by BSEPs. FRT provides a more accurate and automated procedure to prevent breaches of the requirements of the GRA and supports responsible gambling objectives by ensuring BSEPs do not access gaming facilities.

FRT collects a digital image of an individual's face and extracts distinctive features to create a biometric template. FRT will operate by monitoring entry points and cross-referencing individuals with SEP, TABCare and banned patrons included in Bendigo RSL's self-exclusion register and database of excluded individuals (**Exclusion List**).

Because the technology operates in real time, it can immediately flag individuals and notify staff, allowing prompt action to prevent them from gaining access to the gaming floor.

Biometric information and biometric templates are captured under the PA as sensitive information and is therefore afforded a higher level of protection than ordinary personal information in relation to the collection and use of such information.

This PIA will assess how Bendigo RSL can adopt the use of FRT against the requirements set out in the Australian Privacy Principles (**APP**) as it relates to sensitive information.

Bendigo RSL have chosen Ottica as the chosen third-party supplier to install and service the technology.

Scope of this privacy impact assessment

This PIA assesses the key APPs to support the appropriate collection and use of sensitive information in the context of biometric data handling when using FRT, including:

- *Necessity and proportionality (APP 3*)

  This limits the collection of personal information to only what is reasonably necessary for an organisation's functions or activities and in the case of sensitive information, only if the individual consents.
- *Consent and transparency (APP 3 and 5)*

Proactive steps must be taken to sufficiently notify individuals their personal information is being collected and they must be given an opportunity to consent.

- *Governance (APP 1)*

  Organisations choosing to implement FRT must have clear practices and policies for privacy risk management that are regularly reviewed.

- *Accuracy and bias (APP 10)*

  Reasonable steps must be taken to ensure that the biometric data it uses and collects is accurate and address any risks of bias.

This PIA does not cover:

- The technical development of the FRT system by Ottica. This includes technical specifications, system architecture, and other non-privacy-related functionalities.

- Privacy measures relating to personal information already held by Bendigo RSL – including in connection with BSEPs - such as consent records, photographs and identification documents of BSEPs which are unaffected by the introduction of FRT.

Legal authority

Bendigo RSL is authorised under the GRA to maintain a self-exclusion program designed to prevent self-excluded patrons (**SEPs**) from entering gaming areas. To comply with this requirement, they may collect personal information including photographs, signatures, identification documents, and, in the case of banned individuals, additional data such as entry log details and photographic images.

The use of FRT is not legally mandated under the GRA. The legal authority to use FRT is therefore reliant on compliance with the APPs.

Stakeholder consultation

The Program is proposed to be adopted for a trial period during which Patron feedback will be considered as to whether the Program will remain in utilisation. The Hon. Enver Erdogan MLC as the Victorian minister for Casino, Gaming and Liquor Regulation, has indicated that as part of the Victorian Governments commitment to responsible gambling, a trial of facial recognition technology in licensed gambling venues is due in 2026/27. If deemed successful, this technology may become mandatory for licensed gambling venues in Victoria.

Part 2 – Privacy analysis

Identify the information elements

	Question	*Response*
1	**Does the program involve information other than personal information that has the potential to identify individuals?**	Yes (see below)
2	**Does the program involve sensitive information (as defined under Schedule 1 of the PDP Act)?**	Biometric data is sensitive information under the *Privacy Act 1988* (Cth) (**PA**). FRT integrated with the existing CCTV system (FRT-capable cameras) captures individuals' biometric data or facial geometry to generate facial templates, which are then compared against images of BSEPs stored in a database on the Premises.

Collection of personal information

3	**Is all the sensitive information collected necessary for the program?**	The Program collects (briefly) biometric data of all Patrons attending the Premises to compare against the Exclusion List. The purpose of the Program is to match Patrons against the Exclusion List, and therefore all collection is necessary for the Program.
4	**Does the organisation need to collect information that identifies an individual for the purposes of the program, or can individuals remain anonymous?**	The Program information needs to be compared against the Exclusion List and therefore connects to identity.
5	**Is the sensitive information collected directly from the individual?**	Yes. FRT Capable Cameras will obtain biometric data directly from an attending Patron.
6	**Will the individual be notified about the collection of their sensitive information?**	Individuals will be notified their biometric data will be collected by way of notices placed at every entry point to the Premises.
7	**Will any sensitive information about the individual be collected indirectly from another source?**	No.

Security of personal information

8	**Are there security measures in place (existing or intended) to protect the sensitive information collected and used for this program?**	Information held in Bendigo RSL's authorised database of BSEPs is password protected and accessible to only those staff members authorised to access that information. Biometric data of individuals who are positively matched is retained only as long as required to support the operational purpose. Biometric data is deleted for non-matched individuals. Informaiton is secured through role-based access controls, authentication mechanisms and audit logging.
9	**Where and how will sensitive information be stored?**	Biometric data collected by Bendigo RSL's on-premises server infrastructure is retained only briefly and is deleted immediately after a match is identified. Biometric templates which are not a match to banned and self-excluded patrons are automatically deleted. Biometric information for positive matches are retained to complete operational purposes of collection, after which it is securely deleted or de-identified.
10	**Who will have access to the sensitive information?**	Staff members authorised to access and utilise the biometric templates when a match is identified to any banned or self-excluded patron. *Staff members to be given access will include the General Manager, Assistant Manager, Duty Managers & gaming supervisors.*
11	**Has a separate security risk assessment been completed?**	No

Primary and additional uses and disclosures of personal and sensitive information

12	**Is the personal information (including any sensitive information) involved in this program used or disclosed for the main or primary purpose for which it was collected?**	All information in relation to BSEPs will be used for identification purposes and for enforcement of the ban or exclusion – being the primary purpose of collection. There is no disclosure of the biometric data collected to third parties. Ottica AI does not receive copies of or access personal or biometric information of BSEPs. Any access is limited to system-level administrative access to install, configure, maintain or support the FRT platform at the direction of Bendigo RSL.
13	**Does the program use or disclose personal information (including sensitive information) for a new or additional purpose other than the original purpose of collection?**	No

Transfer and sharing of sensitive information

14	**Will any sensitive information be shared outside of the organisation?**	No.
15	**Will any personal information be transferred outside Victoria?**	No.

Other considerations relating to use and disclosure

16	**Will any data matching occur as part of this program? This includes matching datasets within the program, or matching to other datasets external to the program.**	Yes. Biometric data captured by FRT will be cross-referenced against the images held within an authorised database of BSEPs. Where a match is identified, the associated image is retained for operational and compliance purposes, including enabling authorised staff to identify the individual, provide appropriate support, and take any required action in accordance with self-exclusion or ban requirements. The image is accessible only to authorised staff and is retained only for as long as necessary to support these purposes.

Management of personal information

17	**Is there a document available to the public that sets out the organisation's policies for the management of personal information, such as a privacy policy?**	Yes, a Privacy policy and Facial Recognition Technology and Ethical Data Use policy are available. The documents will be available on the Bendigo RSL website.
18	**Will the document be updated to reflect the new collection or use of personal information for the purposes of this program?**	Yes, the policies will be updated by virtue of the Program.
19	**Is there a way for a person to find out the types of personal information the organisation holds about them? Can an individual find out the purposes for which it is held, and how the organisation collects, holds, uses and discloses that information?**	Yes, by way of signage at the entrance to the premises that incorporates a QR code that links directly to the above policies, via the Bendigo RSL website, and otherwise Patrons may enquire with the Bendigo RSL directly.

Retention and disposal of personal information

20	**How long will the sensitive information be kept for?**	Biometric data used for facial matching is processed temporarily in system memory (RAM) for the purpose of determining whether a match exists and is not written to persistent storage where no match is identified. Where no match is made, the biometric data is immediately discarded and never retained. Where a match is identified, the system does not retain a newly created biometric template. The match references the existing biometric image and template already held within Bendigo RSL's authorised database (for example, BSEPs or banned patrons). No additional biometric data is created or stored as a result of the matching process. In addition, the system generates de-identified analytical data, such as timestamps, age and gender estimations, and confidence metrics. This analytical data does not identify individuals and cannot be used to re-identify a person. It is retained to support operational reporting, system performance monitoring, and compliance activities, including assisting staff with the identification of potential minors.
21	**How will sensitive information be destroyed once it is no longer required?**	Biometric data relating to non-matched individuals is automatically purged from system memory immediately after processing and is never stored. Biometric information relating to matched individuals is removed in accordance with Bendigo RSL's data retention policies once it is no longer required for operational or compliance purposes. Deletion processes are automated and designed to ensure data is securely and irreversibly removed. De-identified analytical data is retained only for as long as necessary to support reporting and compliance objectives and does not contain biometric identifiers or personal information capable of identifying an individual.
22	**As an alternative to destroying sensitive information, will any sensitive information be de-identified once it is no longer required?**	Yes, where appropriate. Biometric information is either securely destroyed when no longer required or, where operationally appropriate, de-identified so it can no longer be linked to an identifiable individual. De-identified analytical data (such as aggregated timestamps and age or gender estimations) may be retained for reporting, compliance, and system performance purposes. No biometric identifiers or facial templates are retained in de-identified datasets.
23	**If applicable, what will happen to sensitive information held by third parties (such as contracted service providers, cloud storage, third party platforms etc.)?**	Not applicable. Sensitive information collected through the FRT program is not disclosed to, stored with, or processed by third parties. All biometric information is stored and processed on Bendigo RSL-controlled infrastructure.

Other considerations

24	**Who can individuals complain to if they have concerns about the handling of their personal information?**	*General Manager. Contactable through office@bendigorsl.com.au or phone (03) 5442 2950 during office hours Monday-Friday.*
25	**Does the organisation have a data breach response plan in place?**	Yes. Ottica AI has a data breach response plan in place. Staff are required to immediately report any suspected or actual data breach or unusual system activity so it can be promptly assessed and appropriate action taken in accordance with the organisation's incident response procedures.
26	**Will any training be provided to staff to ensure the appropriate collection and handling of the personal information collected for this program?**	Existing staff will be given on-the-job training in terms of security and management of the FRT data under the Program. Training from Ottica AI is provided to relevant managers at the time of system installation. This training covers the appropriate use of the FRT system, privacy obligations, and the secure handling and management of information generated under the program.
27	**Will the program be evaluated against its objectives?**	Yes, following a 6-month trial period of implementation.
28	**Does the program comply with the organisation's other information handling or information management policies?**	Yes, subject to those policies being updated.
29	**Will this PIA be published?**	Yes.

Part 3 – Privacy risk assessment

	Description of risk	*Accept*	*Risk management strategy*	*Comments*
1	Consider whether the method of collection is fair and not unreasonably intrusive	YES	Information is collected directly and discretely via FRT by cameras on entry following there being visual signage confirming the use of the technology.	No alternative collection means available.
2	If there are inadequate or no security measures in place, consider whether there is a risk that the information will not be properly protected, leading to loss, misuse, or unauthorised access, modification or disclosure	YES	Access to sensitive information is limited to authorised Bendigo RSL personnel. Existing security measures are considered adequate to protect against unauthorised access or disclosure.	Existing security measures are adequate to protect against unauthorised access or disclosure, given the data is immediately and automatically deleted.
3	If engaging third parties such as contracted service providers, consider whether there are arrangements in place to allow access and correction of personal information held by third parties. If not, there may be a risk that individuals cannot access or correct their personal information.	YES	Ottica AI does not hold, retain, or control personal or biometric information collected through the FRT program. As no personal information is held by third parties, there is no risk that individuals would be unable to access or correct their personal information due to third-party arrangements.	As there is no retention or control by third parties, there is no material risk.

4	If there are no arrangements in place relating to third parties' retention and disposal of personal information, consider whether there is a risk that personal information will be held indefinitely.	YES	Ottica AI undertakes regular testing of the FRT system to monitor performance and accuracy, including reviewing match confidence thresholds and analysing system outcomes to identify potential false positives and false negatives. Testing is conducted using controlled datasets and operational performance metrics to ensure the system operates as intended. System configuration settings are reviewed and adjusted where required to support appropriate accuracy levels and reduce the risk of incorrect matches. The FRT system is used as a decision-support tool, with final decisions made by trained staff, which further mitigates the impact of any potential inaccuracies.	As there is no retention or control by third parties, there is no material risk.

Part 4 – Assessment and Conclusion

This part is a summary of the four key Australian Privacy Principles (**APPs**) identified in Part 1 *Scope of the Privacy Impact Assessment*. It provides an analysis of the key privacy elements impacted by the proposed program to introduce FRT at the Premises. Special attention is given to whether the project aligns with the requirements of the *Privacy Act 1988* (**the PA**) by having acceptable privacy outcomes.

APP	*Description*	*Assessment*	*Conclusion*
1	Governance: open and transparent management of personal information. AP1 imposes the following obligations: • take reasonable steps to ensure compliance with the APPs, any inquiries and complaints (APP 1.2) • have an up-to-date APP Privacy Policy (APP 1.3 and 1.4) • make its Privacy Policy available for free (APP 1.5) and, on request, in a particular form (APP 1.6). **N.B**. from 10 Dec 2026, new obligations are introduced for entities who use a computer program to use personal information to make decisions (APPs 1.7, 1.8, 1.9).	The application of FRT is limited in scope to managing legal obligations to prevent access to BSEPs. It is not used for general surveillance or to monitor patrons. To protect the privacy of those individuals who are not banned or self-excluded, Bendigo RSL's proposed FRT system employs the following mechanisms: • **Anonymous Tagging** Unless Patrons are registered in its authorised database, their facial image is tagged as anonymous within the FRT system. This ensures their identity remains protected, and their facial features are not linked to any personally identifiable information. Therefore, individuals not subject to monitoring retain their anonymity and are not identifiable by the system. • **Analytics and Reporting** Any anonymised and aggregated data derived from the FRT system may be used solely for internal analysis to evaluate operational effectiveness. Importantly, these analytics do not include or reveal any personally identifiable information, safeguarding the confidentiality of all individuals	Bendigo RSL regularly monitors and reviews it privacy policies - available to review on its website - to assess its compliance with legal requirements and industry best practice The approach to implementing FRT emphasizes privacy and transparency. The chosen technology is designed to protect the privacy of individuals who do not need to be monitored, ensuring their anonymity is maintained. This is achieved by using aggregated and anonymized data for analytics, safeguarding personal information. Regular monitoring and review processes are in. These mechanisms are intended to collectively support transparency, accountability, and continuous improvement in the use of FRT

3	Necessity and proportionality: collecting personal information that is reasonably necessary and sensitive information by consent. AP3 imposes the following obligations: • must only collect personal information which is reasonably necessary (APP 3.1, 3.2) • individuals must consent to the collection of their sensitive information (APP 3.3)	Bendigo RSL has legal obligations to maintain and enforce the SEP under the GRA, and, in the case of banned individuals it's necessary to prevent these persons from entering the Premises. The Premises has in excess of 300 BSEPs, which is arguably implausible to be enforced by manual means. The Program is reasonably necessary to ensure compliance with the GRA and manage responsible gambling obligations. Informed and current consent is obtained by virtue of voluntary attendance after visual signage is displayed at appropriate entry locations for Patrons.	BSEPs are aware their personal information is collected and they're prohibited from entering. FRT is an additional measure to enforce this, and all Patrons will be notified of its use at the entrance to the Premises. Given the number of BSEPs, the use of FRT provides an effective means of identifying individuals more accurately to prevent potential breaches of the GRA. The proportionality of using FRT directly supports the goal of compliance with the GRA. FRT strengthens the integrity of the SEP and outweighs the extent of any privacy impacts for the purposes of the Program.
3 and 5	Consent and transparency: informed consent is required for collection of biometric data. AP5 imposes the following obligations: • Collection notices must be transparent and give individuals opportunity to provide consent (APP 5.2) • Give individuals an alternative process if they do not consent	Bendigo RSL will display prominent signage at all entry points informing all Patrons that if they wish to enter the Premises, FRT is in operation. Patrons who do not consent can chose not to patronise the Premises.	The signage will include a QR code that links directly to Bendigo RSL's privacy policies about the collection, use, and management of their personal information, including biometric data. Further consent from SEPs will be obtained through explicit agreements as part of SEP registrations.
10	Accuracy and bias: personal information collected, used and disclosed must be accurate, up to date and relevant. AP10 imposes the following obligations: • Information contained in the database of BSEPs must be	Bendigo RSL intends adopting an FRT system that employs industry-standard encryption for data processing to create biometric templates direct from Patrons. These templates are held temporarily for the purpose only of cross-referencing patrons from the banned and self-excluded database and immediately deleted after use.	The FRT system selected reflects our approach to maintaining a secure and responsible use of FRT to comply with APP requirements.

	accurate and up to date. • Regularly test the FRT system for data quality practices to avoid bias and through inaccurate matches.		

Part 5 – Action items, board approval and documents

This part details any action items identified, endorsement of the PIA, and document information. Refer to **Part 4** of the PIA Guide for more information.

Action items

	Action	*Timeframe*
1	Re-draft Privacy Policy and Facial Recognition Technology and Ethical Data Use policy	Prior to implementation
2	Training all staff on updates to privacy legislation and collection of biometric data	Prior to implementation
3	Allocation of appropriate individuals to access FRT system	Prior to implementation

Board approval

Approval of the Bendigo RSL Board will be obtained prior to implementation of the Program.

Document information

Document title	Privacy Impact Assessment
Document owner	Bendigo RSL Sub-Branch Inc.
Document distribution	Published.
Related documents	Privacy Policy and Facial Recognition Technology and Ethical Data Use policy
Next review	6 months from publication.
Document version	1.0