From: OIA <oia@selwyn.govt.nz>
Sent on: Wednesday, March 5, 2025 2:40:17 AM
To: marysagen@gmail.com
Subject: RE: AI use at swimming pool
Attachments: Drowning Prevention System - Privacy Impact Assessment Final.pdf (1.16 MB)

Dear Mary,

Official information request for pursuant to the Local Government Official Information and Meetings Act (LGOIMA)

We refer to your official information request dated 4 February 2025 for information relating to AI use at swimming pool.

Please see response relating to your request:

-
Question: What kind of AI technology is in use and what company was it procured from?
Answer: The AI technology is provided by MSK Management Group, Australia.
The cameras and system:

- Analyse swimmers' movements for potential incidents
- Can see through water for a 360 view above and below
- Help eliminate blind spots – up to 4x as many vantage points per lifeguard
- Provide smartwatch alerts to help accelerate response times and spot incidents before they escalate

-
Question: What is the cost of the cameras and their installation? What are the predicted ongoing operation and maintenance costs? How do these compare to hiring more lifeguards?
Answer: The budget for the one-off implementation is $160,000, with ongoing licensing and support fees estimated at $80,000 per year.
Hiring an additional lifeguard per shift would be approximately $145,000 per year ongoing. Note, this system has been implemented to provide supplementary support to lifeguarding activities.

-
Question: Have you written a thorough privacy impact assessment and is it available for viewing?
Answer: We have attached a copy of the privacy impact assessment. We have redacted certain parts of the document due to cyber security reasons. This is to protect the privacy of natural persons (7 (2)(a)), to avoid prejudice and protect the health and safety of members of the public (7(2)(d)), to protect information which is subject to obligation of confidence that would likely damage public interest 7(2)(c)(ii), and to ca
out commercial activities without prejudice or disadvantage (7(2)(h)).

-
Question: How are pool users identified that AI is in use and are you getting their informed consent?
Answer: The aquatic centre has had cameras in use for some time with associated signage onsite.
Note, the drowning prevention system is not used to record details to identify people but is based on identifying swimmer movements relating to possible drowning behaviours.

-
Question: What would you say to your users who experience increased anxiety with the increased implementation and use of CCTV paired with AI tech?
Answer: The Selwyn District Council takes privacy seriously. We want to assure people that the recordings are not connected to any facial or other recognition systems.
The recording capture is only used by the system to identify possible signs of a swimmer in distress, not record any details that could identify people.
No staff members have access to the recordings, which are deleted after 7 days.

If you wish to discuss this decision with us, please feel free to contact us at oia@selwyn.govt.nz.

You have the right to seek an investigation and review by the Ombudsman of this decision. Information about how to make a complaint is available at www.ombudsman.parliament.nz or freephone 0800 802 602.

Yours sincerely,
LGOIMA Team
Selwyn District Council

Drowning Prevention System Privacy Impact Assessment Report

August 2024

Privacy Impact Assessment Report – Contents

1. Project summary

This Privacy Impact Assessment is for the AI Lifeguard project for the installation of AI camera technology to detect drowning or distress in the Selwyn Aquatic Centre and possibly extending to other pools in the Selwyn district. This technology will add an additional level of supervision to the pool areas where glare, visibility and supervision issues were identified as the main contributing factors for not identifying the problem in a previous incident. It will provide automatic alerts to Lifeguards on the floor via smart watches for prompt review and management.

The Privacy Impact Assessment (PIA) is required to review the potential privacy risks around identification and storage of data associated to private information collected through the cameras. By evaluating the potential impact on individuals' privacy rights, the Council can consider the extent to which the AI Lifeguard technology complies with legal and regulatory requirements and identify mitigants to address any potential areas of non-compliance or other concerns.

The PIA is being completed during the implementation phase of the project.

The project is seeking to implement the AI Lifeguard in the Selwyn Aquatic Centre, and if successful will be sought to extend to other pools within the Selwyn district.

2. Scope of the PIA

2.1 Scope

The Privacy Impact Assessment for the AI Lifeguard project initially starts at the Selwyn Aquatic Centre but will cover any pool this system will be installed at within Selwyn. It will look at:

1. **Technology Implementation**: Evaluation of the AI camera technology being installed to detect drowning or distress in pools.
2. **Data Collection**: Assessment of the personal information gathered through the cameras.
3. **Legal Compliance**: Review of how the technology aligns with legal and regulatory requirements related to privacy.
4. **Risk Identification**: Analysis of potential privacy risks associated with the use of AI cameras in pool areas.
5. **Mitigation Strategies**: Identification of measures to address any areas of non-compliance or privacy concerns.
6. **Impact on Individuals**: Evaluation of how the technology might affect individuals' privacy rights.

The PIA will aim to ensure the Council's processes are designed and implemented in a way that protects individuals' privacy while allowing the AI Lifeguard system to function effectively for improved pool safety. It will cover:

1. **Use**: How the collected data will be utilised, particularly in sending automatic alerts to lifeguards via smart watches
2. **Storage**: Methods and systems for storing the data captured by the AI cameras.
3. **Access and Security**: Who will have access to the collected information and under what circumstances
4. **Retention**: How long the data will be kept and policies governing data retention.
5. **Disposal**: Procedures for securely disposing of the data when it's no longer needed.

2.2 The process

The PIA has been put in place during project implementation. Information has been gathered and reviewed as it was assessed for suitability. The project team have been involved in bringing this information together along with consultation with the supplier.

Personnel / Team	Touchpoints
Selwyn Aquatic Centre Staff	Use of AI Lifeguard
Information Management Team	Storing of data if required, R&D
Digital Services Team	Support of IT and security of system
Legal Services	Review of PIA

2.3 Explain the scope and process

AI Lifeguard is an artificial intelligence system designed to monitor swimming areas and assist in drowning prevention. The system uses cameras and sensors to collect real-time data on swimmers and environmental conditions. The rationale for the scope of the PIA has been centred around concern and perception that the AI Lifeguard system collects and processes visual imagery of swimmers in the pool areas that could be identifiable, how we deal with this and protect individuals' privacy.

The AI Lifeguard collects and processes the following data:

- Visual imagery of swimmers in the pool areas
- Depth of pool information
- Swimmer behaviour patterns

This data is processed in real-time by the AI algorithm to identify potential drowning risks. Potential privacy risks include:

- Unauthorised access to visual data of swimmers
- Misuse of collected data for purposes beyond drowning prevention
- Inaccurate identification of drowning risks leading to unnecessary interventions
- Long-term storage of personal data without consent

3. Personal information

4. Privacy assessment

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
1	Principle 1 - Purpose of the collection of personal information Only collect personal information if you really need it	The AI Lifeguard will constantly record, via video with low pixelation, individuals within the swimming pool. Each individual will be assigned a unique identifier which remains with them whilst they are in the pool. The unique identifier is not connected to any biometric database that could connect any identifying information. Features cannot identify an individual. Each time a swimmer leaves the pool they lose their unique identifier, and they gain a new one when they go back in.	**Compliant.** The system collects only video data necessary for pool safety monitoring. Low pixelation and temporary unique identifiers are used to minimize personal data collection. No biometric or personally identifiable information is stored or linked to the video data. Identifiers are reset when swimmers exit and re-enter the pool, preventing long-term tracking.	

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
2	Principle 2 – Source of personal information Get it directly from the people concerned wherever possible	The information collected is video evidence of people movement but without identifying features, instead there are unique identifiers allocated to each swimmer as they enter into the pool for the AI to study their pool behaviour for health and safety risks. The information is collected to build up intelligence of such behaviour and to teach the AI over time what behaviour is deemed safe or not. All information is stored on servers within our own location and not in the cloud or taken offsite at all. Although the system directly collects information from individuals as they use the pool, the indirect nature of video surveillance without explicit consent raises some considerations. We will mitigate these with: • Ensuring no identifying features are captured (low pixilation/blur) • Unique identifiers are temporary • Data is used for safety purposes only • Local storage enhances security • Media Release and public notices informing movements are being recorded for safety purposes and are not personally identifiable.	**Compliant with recommendations:** The data collection method (video 'surveillance') is indirect, but necessary for the safety purpose. Measures are in place to minimise personal data collection and protect privacy: • No identifying features are captured • Unique identifiers are temporary and not linked to personal information • Data is used solely for safety and AI learning purposes • Information is stored locally, enhancing security and control These considerations balance the principle's intent with the practical needs of the safety system.	

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
3	Principle 3 – Collection of information from subject Tell them what information you are collecting, what you're going to do with it, whether it's voluntary, and the consequences if they don't provide it.	Public notices on website, social media channels, media releases	Selwyn District Council - Privacy Policy – update this webpage on Privacy Update public facing Privacy Policy to include use of video for health and safety purposes	
4	Principle 4 – Manner of collection of personal information	Video recordings are collected of all swimmers and pool goers whilst in the pool, ensuring no identifying features (low pixilation/blur)	**Compliant.** The system appears to collect information in a fair and minimally intrusive manner: • Video collection is limited to the pool area, where safety monitoring is expected. • No identifiable personal information is displayed or stored.	

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
5	Principle 5 – Storage and security of personal information	Storage of the videos will be onsite on servers held on premise within a limited network. There is no access to these recordings. Only the Chief Digital Officer can request any access. 7(2)(a), 7(2)(c)(ii), (7(2)(d)), (7(2)(h) [redacted] The data retention and deletion policy indicates that we will retain only data for up to 7 days, after which all data will be securely deleted. Lifeguard training on how to use the smart watch will be provided to staff both online and in-person. For new Lifeguards, it will become part of their standard onboarding training.	**Compliant with recommendations:** • External compliance monitoring ensures ongoing data protection. • No personally identifiable information is transmitted or stored. • Staff training is planned for proper system management. To fully comply and strengthen security: 1. Clearly define and document who has access to videos and software. 2. Implement a robust permission system for software access. 3. Establish a regular training schedule and maintain records. 4. Conduct regular security audits and penetration testing.	

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
6	Principle 6 – Access to personal information	There is no personal information that is identifiable for someone to request to see. However, if an incident happens in the pool, and the movements need to be analysed for the investigation, the process for dealing with these requests for access will be made via the Chief Digital Officer only.	**Compliant with recommendations:** Document a process for accessing relevant information in case of an incident – via the Chief Digital Officer only.	
7	Principle 7 – Correction of personal information	There is no personal information that is identifiable to an individual for corrections to be made.	**Compliant.**	
8	Principle 8 – Accuracy etc. of personal information to be checked before use Make sure personal information is correct, relevant and up to date before you use it	There is no personal information that is identifiable to an individual that are used in this way. Whilst the information collected through the AI camera does not identify individuals and collect personal information, there is a possibility that the AI may evolve to a point where personal features are more prominent and therefore distinguishable. To mitigate this, the vendor has intentionally chosen to keep the video picture detail at 5 megapixels which maintains the level of detail. Approx. 3 year shelf life for the cameras.	**Compliant with recommendations:** Implement a regular 6-monthly review process for the AI system, focusing on: • Any changes in data collection or processing that might lead to personal identification • Adherence to the intended 5 megapixel resolution • Any unintended developments in AI capabilities that could compromise privacy.	

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
9	Principle 9 – Not to keep personal information for longer than necessary	The data collected through the AI cameras will be kept on on-premises servers for a length of 7 days. An automatic deletion will be set up at 7 Days to remove the data from the server.		
10	Principle 10 – Limits on use of personal information	The information the system presents is human figures with no close-up identifying features.	Compliant with recommendation: Implement regular audits to ensure the system and its data are not being used for any unintended purposes. Provide training to staff on the importance of using the system only for its intended purpose. Establish a process for reviewing and approving any potential new uses of the system or its data, should they arise in the future. Implement technical controls to prevent unauthorised access or extraction of data that could lead to use for other purposes.	

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
11	Principle 11 – Limits on disclosure of personal information	Video that possibly could identify an individual, due to circumstances (few numbers present, and location) is used to monitor pool behaviour, but is not intended to disclose. Noting that no staff have access to these recordings. If numbers are few in the pool and associated with knowledge of who these individuals present are, can individuals be identified, however this is not captured within the software and so information is kept totally anonymised. And this information is not presented on screen to staff either.		
12	Principle 12 – Disclosing information outside New Zealand Only share information with an agency outside New Zealand if the information will be protected	7(2)(a), 7(2)(c)(ii), (7(2)(d)), (7(2)(h) [redacted] They adhere to Australian Privacy Principles(APP), Data Protection Act 2018 (DPA 2018) and the General Data Protection Regulation 2016/679 (refer to 4.1.1 in Terms and Conditions. As per 4.2.7 all data must be anonymised, and 4.1.3 any videos are stored for a period of up to 7 days only.		
13	Principle 13 – Unique identifiers Only assign unique identifiers where permitted	Swimmers receive a unique identifier (UUID) upon entry to the pool; a new UUID is assigned if they exit and re-enter. This reduces any identifiable information.		

Summary / Conclusions

The AI Lifeguard project represents a sophisticated approach to pool safety that carefully balances technological innovation with robust privacy protection. By implementing a system that uses low-pixelation video with temporary unique identifiers, the project ensures minimal personal data collection while maximizing safety monitoring. The technology intentionally prevents individual identification through strategic design choices such as blurring swimmer features, using temporary unique identifiers that reset upon pool exit, and storing data locally for only 7 days.

Critically, the system's primary purpose remains focused on drowning prevention, with multiple layers of privacy safeguards including limited access, local server storage, external compliance monitoring, and planned staff training to ensure the technology is used exclusively for its intended safety purpose.

5. Risk assessment

This section describes the privacy risks you've identified through the PIA process and how you propose to mitigate and manage those risks. It can be useful to link this back to the privacy principles to show why these risks and the proposed actions are relevant.

Note: A PIA doesn't set out to identify and eliminate every possible privacy risk: its role is to identify genuine risks that are not unreasonably small or remote.

Categorise your proposed actions

In some cases, it may be helpful to categorise these actions into areas such as:

- governance
- people
- process
- technology

Categorising the proposed controls in this way helps to define where within the organisation they will be managed.

Add a narrative summary of your risk assessment and options for mitigating those risks here.

Alternatively, attach a separate risk assessment document, such as one modelled on the template in Appendix C. If you don't want to attach the whole document, you can cut and paste the relevant information into this section.

Document the risks in line with any existing risk management processes your organisation has – it will be more efficient than trying to run a separate process.

6. Recommendations to minimise impact on privacy

Summarise the recommendations to minimise the impact on privacy based on your risk assessment

Ref	Recommendation	Agreed Y/N
R-001	Implement regular system audits to ensure data is used only for its intended purpose	
R-002	Enhance data minimisation protocols, especially during low-occupancy periods	
R-003	Update public-facing privacy policies to include information about video usage for health and safety purposes	

7. Action plan

This section of the report should describe what actions are being taken (whether short or long term) and how they'll be monitored. There may also be links to other processes in the organisation. For example, a proposed action might relate to security controls (such as restricting access to a system). This will then link in with security processes in the organisation.

Reporting on the outcome of the mitigation may be necessary. If the PIA is being performed as part of a project, then the project is likely to require some reporting on their implementation as part of governance arrangements. Once the project is completed, any on-going privacy monitoring should be incorporated into normal business operations.

In the case of a particularly long or complex programme of work, the PIA may need to be reviewed a number of times to ensure that it continues to be relevant. This section should describe how this will be achieved.

Ref	Agreed action	Who is responsible	Completion Date
A-001	Develop and implement a 6-monthly review process for the AI system, focusing on: • Changes in data collection or processing that might lead to personal identification • Adherence to the intended 5 megapixel resolution • Unintended developments in AI capabilities that could compromise privacy		
A-002	Create a documented process for accessing relevant information in case of an incident – note only the Chief Digital Officer can request this.		
A-003	Develop and distribute media releases and public notices informing users that movements are being recorded for safety purposes and are not personally identifiable.	Information release out to external media. Post on social media channels (Facebook, LinkedIn, and YouTube). Put information up on the SDC website.	
A-004	Update the Selwyn District Council Privacy Policy webpage to include information about video usage for health and safety purposes		
A-005	Install rolling electronic notices within the pool area and other static notices to inform users about the AI Lifeguard system		

A-006	Establish a regular training schedule for lifeguard staff and maintain these training records.	To be included in current lifeguard training	
A-007	Check if implementation of a data minimization protocol for low-occupancy periods to further reduce the risk of individual identification is required.		
A-008	Develop a process for regular audits to ensure the system and its data are not being used for any unintended purposes.		