



greater WELLINGTON

REGIONAL COUNCIL

Te Pane Matua Taiao

Privacy Impact Assessment

Public Transport Camera Surveillance

6th July 2018

Contents

Contents.....	1
Glossary.....	3
Related Documents.....	3
1 Executive Summary.....	4
1.1 Inherent Risk Level.....	4
1.2 Residual Risk Level.....	4
2 Project Summary.....	6
2.1 Overview.....	6
2.2 Rail Services.....	6
2.3 Bus Services.....	6
2.4 Ferry Services.....	7
3 Privacy Impact Assessment (PIA).....	8
3.1 Scope.....	8
3.2 Rational for Completion.....	8
3.3 Development Process.....	8
3.4 Structure.....	8
4 Rail Services.....	9
4.1 Collection of Personal Information.....	9
4.2 Use of Personal Information.....	11
4.3 Disclosure of Personal Information.....	12
4.4 Security of Personal Information.....	14
4.5 Retention and Disposal of Personal Information.....	14
4.6 Unique Identifiers.....	15
4.7 Risk Assessment.....	16
4.8 Action Plan.....	19
5 Bus Services.....	21
5.1 Collection of Personal Information.....	21
5.2 Use of Personal Information.....	22
5.3 Disclosure of Personal Information.....	22
5.4 Security of Personal Information.....	23
5.5 Retention and Disposal of Personal Information.....	23
5.6 Unique Identifiers.....	23
5.7 Risk Assessment.....	24
5.8 Action Plan.....	26
6 Bus Hubs.....	27
6.1 Collection of Personal Information.....	27

6.2	Use of Personal Information	28
6.3	Disclosure of Personal Information	28
6.4	Security of Personal Information	29
6.5	Retention and Disposal of Personal Information.....	29
6.6	Unique Identifiers	30
6.7	Risk Assessment	31
6.8	Action Plan	34
7	Authorisation	36

Glossary

Term	Meaning
Council	Greater Wellington Regional Council
GWRC	Greater Wellington Regional Council
GWRL	Greater Wellington Rail XX
PIA	Privacy Impact Assessment
PTOM	Public Transport Operating Model
RMC	Rail Monitoring Centre based at Wellington Railway Station
SCC	Service Control Centre based at Wellington Railway Station

Related Documents

The following documents are related to this privacy impact assessment:

Title	Author
180502_3889_Bus Hubs High Level Design Showing Canopy	Isthmus
Conditions of Carriage (https://www.metlink.org.nz/tickets-and-fares/conditions-of-travel/)	GWRC
Current GWRC Privacy Statement (http://www.gw.govt.nz/privacy-statement/)	GWRC
Current Metlink Privacy Statement (https://www.metlink.org.nz/privacy/)	GWRC
Draft Camera Page for Website	TwoBlackLabs
Draft Privacy Statement	KensingtonSwan
Draft PT Group camera surveillance system policy	TwoBlackLabs
Draft Red Wolf Agreement for Supply of Camera Surveillance System and Associated Services	GWRC
PTO584 – CCTV and Audio Installation Maintenance Services – Dec 2017	GWRC
PTO416 – Partnering Contract	GWRC
Bus Operators Contract	GWRC
CCTV Access Request Form April 2017	Transdev
CCTV RMTU Interim Agreement	KiwiRail
LOA Police and Transdev 11072017	Transdev
Monthly Performance Report May 2018	Transdev
TDW Security Management Plan – Draft Feb 2018	Transdev

1 Executive Summary

1.1 Inherent Risk Level

The privacy impact assessment (PIA) has identified 43 privacy risks as shown below. There are eight risks rated as high and twenty-one rated as medium assuming all current controls are functioning effectively.

The high risks relate to four key themes:

- Inadequate signage advising individuals that they are under surveillance – A03, C03
- Disclosure of footage without authorisation from GWRC / GWRL – A13, A14, A15, A16, C13
- Security of footage within the existing camera surveillance system operating on the rail network – A6
- Handling of privacy requests – A07, B04, C07.

Likelihood	Almost Certain	A07, B04, C07	A04, A19, B01, C04, C16	A03, A13, A14, A15, A16, C03, C13		
	Likely	B08	B02	A05, A09, B05, B07, C05, C09, C10	A06	
	Unlikely		C12	A01, A10, A11, B06, C06		
	Highly Unlikely		A12, B03	A02, A17, A18, C01, C02, C11, C14, C15		
	Rare			A08, C08		
		Individual	Single	Moderate	Major	Extreme
		Consequence				

1.2 Residual Risk Level

If all the recommended additional controls are implemented and are functioning effectively the risk level reduces as shown below. Once the additional controls are implemented there are no risks rated as high and one remaining rated as medium. The one remaining medium risk, B04, relates to individuals incorrectly requesting footage obtained whilst aboard a bus from GWRC. These requests need to be transferred to the relevant Bus Operator. It is proposed that GWRC take steps to minimise the number of these requests however as individuals identify Metlink as the provider of the bus services it is expected that a large number will still be received.

Likelihood	Almost Certain	B04				
	Likely					
	Unlikely		A03, A05, B01, B02, C03, C05			
	Highly Unlikely	A04, B08, C04	A09, A12, A14, B03, B05, C09, C12	A01, A02, A06, A10, A13, B06, B07, C01, C02, C06, C10, C13		
	Rare	A07, A15, A16, C07	A19, C16	A08, A11, A17, A18, C08, C11, C14, C15		
		Individual	Single	Moderate	Major	Extreme
		Consequence				

2 Project Summary

2.1 Overview

The new Public Transport Operating Model (PTOM) passed into legislation in 2013 and created a strategic change in the way Wellington's public transport system is planned and procured by Greater Wellington Regional Council (GWRC). PTOM aims to build long-term commercial partnerships between regional authorities and public transport operators, to improve services and grow patronage.

Journeys on buses, trains and ferries in the Wellington region are forecast to increase from 38 million to 42 million trips a year, between now and 2024.

2.2 Rail Services

GWRC funds rails services on four key lines throughout the region:

- Hutt Valley Line
- Johnsonville Line
- Kapiti Line
- Wairarapa Line.

Wellington's rail services were the first to go through the new PTOM contract process. Transdev Wellington were awarded the contract and took over operating the network on the 3rd July 2016.

Camera surveillance is utilised across the rail services including:

- At railway stations, carparks, bridges and subways
- Within passenger carriages on trains
- On the front and rear of trains
- At the Rail Monitoring Centre
- Use of a very limited number of bodycams.

2.3 Bus Services

GWRC fund bus services across the entire region. These are split into several geographic regions:

- Wellington city
- Wairarapa
- Hutt Valley
- Porirua
- Kapiti

The bus services have recently been through the new PTOM contract process. The bus changes are being rolled out in three phases – in the Wairarapa from 30 April 2018, the Hutt Valley from 17 June 2018 and in Wellington, Porirua and Kapiti from 15 July 2018.

As part of the changes to bus services some bus routes are being changed. Eight new Bus Hubs are being introduced across Wellington city as part of the changes. These connect buses from outer suburbs with main routes. Each Bus Hub consists of several bus shelters. The Bus Hubs are located at:

- Bus Interchange at Wellington Station
- Courtenay Place – near Allen Street
- Johnsonville – Moorefield Road and Johnsonville Station
- Kilbirnie – Evans Bay Parade
- Miramar – Miramar Avenue
- Newtown – outside the Regional Hospital
- Karori Tunnel – city side on Glenmore Street
- Brooklyn – Cleveland Street.

Camera surveillance is utilised across the bus services including:

- At the new Bus Hubs¹
- Onboard all buses
- Externally on all buses.

2.4 Ferry Services

Two harbour ferries, the City Cat and the Cobar Cat run peak and off peak commuter services between Days Bay, Queens Wharf and Seatoun. These are operated by East West Ferries Limited.

There is currently no camera surveillance in operation on ferry services.

¹ Camera surveillance system at the Bus Interchange at Wellington Station is owned and operated by Wellington City Council (WCC)

3 Privacy Impact Assessment (PIA)

3.1 Scope

This Privacy Impact Assessment (PIA) covers the camera surveillance usage across GWRC's Public Transport. This PIA will consider the entire information lifecycle including:

- Collection practices
- Use of personal information
- Disclosure of personal information
- Security of personal information
- Retention and disposal of personal information.

This PIA does not cover the ferry services as currently no camera surveillance is in operation on these services.

This PIA also does not cover the camera surveillance operations of the operators as these are not the responsibility of GWRC.

3.2 Rational for Completion

GWRC has recently reviewed their camera surveillance usage at a high level across all their areas of responsibility. This review identified that the usage of camera surveillance within the public transport network was a high risk activity unless appropriate controls are implemented.

This PIA has been commissioned to understand the current level of controls in place and to identify any additional controls that could be introduced to further reduce any residual risk.

3.3 Development Process

A review of the collateral relating to the current and proposed operations was undertaken. Collateral included:

- Business requirements
- Build specifications
- Current contracts
- Proposed contracts
- Operating procedures.

Several workshops were also conducted to discuss the information lifecycle for surveillance footage.

3.4 Structure

The parties utilised to provide the various services differs along with the operating procedures and processes. Therefore, the PIA is split into three sections:

- Rail services
- Bus services
- Bus Hubs.

4 Rail Services

4.1 Collection of Personal Information

Most of the stations on the Metlink network are under camera surveillance. The area under surveillance varies per station however it generally includes the following areas:

- Platforms
- Waiting rooms
- Carparks
- Bridges
- Subways
- Train yards.

The cameras only record visual footage and can work in very low light conditions. The cameras operate 24 hours a day, seven days a week. Some of the cameras are fixed on a specific location and others can be swivelled and zoomed by the Surveillance Officers as required.

Cameras also operate on all GWRC trains. There are four cameras located inside each passenger carriage (8 in a two car unit) and one on the front and one on the rear of the train.

The bodyworn cameras in operation are operated by Transdev and are therefore not the responsibility of GWRC or GWRL.

All the cameras and related equipment are owned by GWRL, a subsidiary of GWRC. Red Wolf are responsible for the installation and maintenance of the camera equipment at stations. Transdev are responsible for the maintenance of the cameras installed on the trains, which is subcontracted to Hyundai-Rotem. Transdev are also responsible for the monitoring of the cameras at both the stations and on the trains. Monitoring of the cameras at the stations is subcontracted to Armourguard.

The Public Transport Group Camera Surveillance Policy details that footage is to only be collected for the purposes of:

- Immediately detecting criminal events, objectionable behaviours and safety incidents
- Collecting evidence for prosecution of criminal events
- Monitoring of patterns of travel behaviour in groups of customers where no individual customer is uniquely identifiable
- Ensuring fare revenue is appropriately collected.

The capturing of footage is also used to deter criminal events, objectionable behaviours and safety incidents occurring.



Individuals are made aware that camera surveillance is in operation at the stations, for the purposes of crime prevention and safety, through the inclusion of signage. The signs are highly visible to any person within the area normally being captured as part of the footage. The signs contain both the phone number for Metlink and the website address. Red Wolf are responsible for ensuring that the signs are in place at least every six months and advising GWRC of any that require replacement.

Upon the trains, passengers are made aware that camera surveillance is in operation for the purposes of crime prevention and safety, through the inclusion of signage on the bulk head of each carriage. When the train is busy there is potential that all customers may not be aware that cameras are operating as they are unable to view the signage. Transdev are responsible for ensuring that the signs are in place and replacing any as required.

The GWRC privacy statement is currently being updated and will replace the existing Metlink privacy statement (<https://www.metlink.org.nz/privacy/>) as well as the current GWRC Customer Privacy Policy (<http://www.gw.govt.nz/privacy-statement/>) which provide details about the use of camera surveillance within the rail network.

The new privacy statement is currently in the process of being reviewed by ELT and is expected to be in place within the next month. It details that camera surveillance is in operation and directs individuals to a webpage detailing the locations where surveillance is used and the purposes. This webpage includes details of the camera surveillance operating within the rail network.

If an individual contacts either the Metlink Call Centre or the GWRC Service Centre they are provided details regarding the usage of camera surveillance based on the information contained within the privacy statement or can request a copy of the privacy statement.

The Conditions of Carriage also detail that camera surveillance is in operation and directs individuals to the GWRC privacy statement for further information.

Transdev are responsible for ensuring individuals are made aware that camera surveillance is in operation using bodyworn cameras and that they operate the system. Due to the requirement that the signage indicates the collection purpose and the system operator the signs cannot be developed by GWRC in isolation. The PTOM contract requires each Transdev to develop a privacy statement that covers the bodyworn cameras. GWRC can provide feedback on the privacy statement. GWRC require that Transdev make the privacy statement freely available upon request by any person, this is currently not available.

The Rail Monitoring Centre (RMC) and ticket offices are also under camera surveillance. Therefore, employees of GWRC, Transdev and Armourguard working in these environments are captured in the footage. The Transdev Security Plan details that staff will be advised in writing, and notices posted in staff common areas, to ensure all staff are aware that cameras operate in these areas. However, there is no evidence of these actions currently occurring.

Limited personal information is also collected about the actions of GWRC, Red Wolf, Transdev and Armourguard employees who access the camera surveillance system for monitoring and administrative reasons. The information collected relates to the individual who logged on to the system and the actions they took. This is contained within the logs of the system. The staff are not made aware at the time that their behaviours are being monitored.

4.2 Use of Personal Information

The cameras installed at the stations are monitored 24 hours a day, 7 days a week, by Armourguard Surveillance Officers located in the RMC. The individual cameras are not monitored a hundred percent of the time but rather the operators cycle through them. The Surveillance Officers can control the majority of the cameras and swivel and zoom them in as required to monitor a situation. The Surveillance Officers can view private property utilising the cameras however standard practice is not to do this unless they are following an assailant.

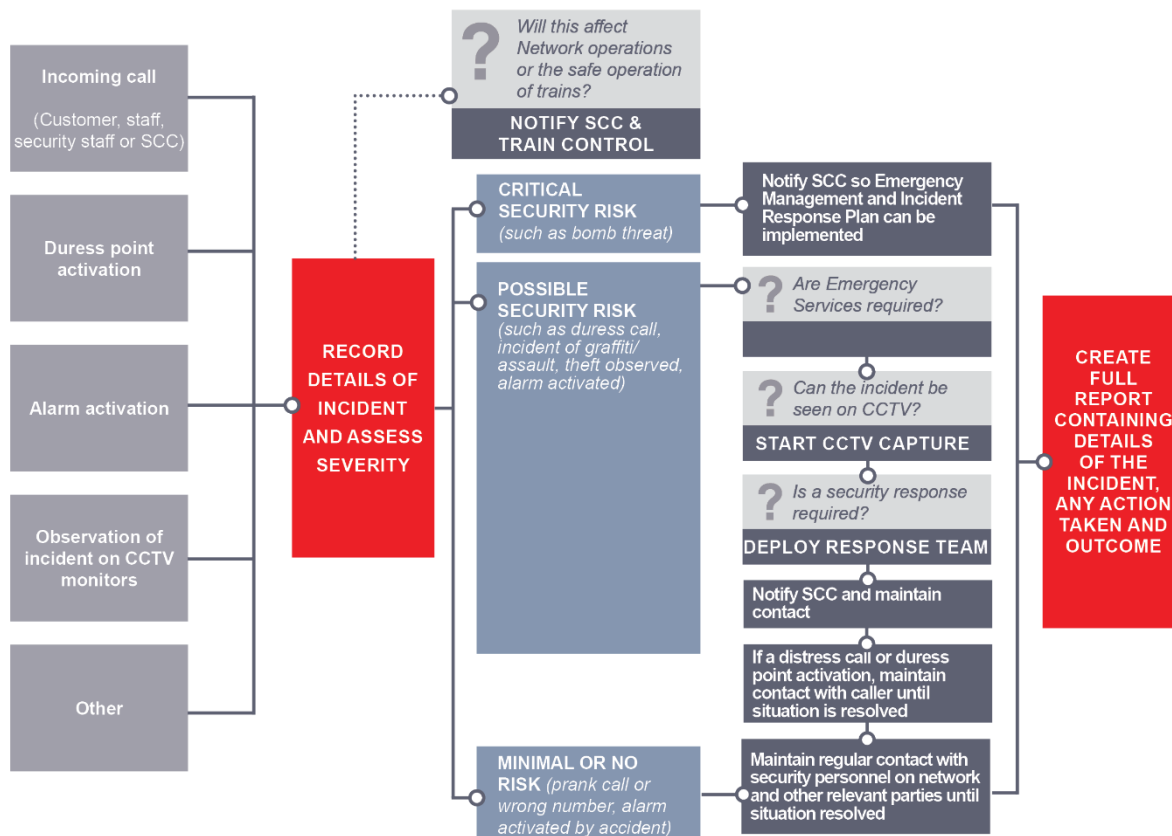
The onboard train cameras can be monitored in real-time by Transdev staff onboard the train on a monitor in the guard's area. There is no ability to view historic footage onboard the train. The process for accessing historic footage involves the Transdev Security Manager removing the drives from the required train, replacing the drives with a spare set and then downloading the footage in the RMC. Historic recorded footage is only accessed by Transdev in the event of an incident / request.

The Transdev contract details that Transdev and their subcontractors must only use footage for the purposes requested by GWRL as specified within the agreed Security Management Plan.

The Public Transport Group Camera Surveillance Policy details that footage can only be used for the purpose for which it was collected. The footage may also only be used, with the prior approval of the Responsible Officer, for the following related purposes:

- Inquiries relating to the investigation of other criminal offences or safety incidents
- Training of security staff and maintenance of the system
- Research, such as into the nature of security incidents, patterns in use or travel behaviour, or evaluation of the operation of particular camera systems.

The Surveillance Officers primarily monitor the rail network for incidents or issues and respond in accordance with the Security Risk Procedure as below.



The Transdev Security Manager or the RMC Surveillance Officers may also review recorded footage in circumstances where they are requested by NZ Police to establish events when dealing with a live situation.

Access to footage of the RMC and ticket offices can only be accessed by the Transdev Chief Operating Officer or the Transdev Security Manager. These feeds are not available to the Surveillance Officers in the RMC.

Regular audits are carried out by the Transdev Security Manager of the records of who accessed the system, copied footage and provided images to external parties. This information is used to identify unauthorised behaviours and to investigate any incidents.

The use of the footage collected by the bodyworm cameras is determined by Transdev.

4.3 Disclosure of Personal Information

The Transdev Security Manager is responsible for ensuring that all staff are aware of and comply with the Public Transport Group Camera Surveillance Policy. Footage must not be copied or removed from the RMC without prior written approval.

The identity of individuals within the footage from the stations is not masked and is visible to anyone within the RMC. All the Surveillance Officers within the RMC are licenced under the Private Security Personnel and Private Investigators Act 2010. Access to the RMC is restricted to authorised personnel, except with written permission from the Security Manager. The public are unable to observe the area as all external windows are frosted.

Limited footage of station cameras is also available to operators within the Service Control Centre (SCC). The identity of individuals within the footage is not masked. Staff within the SCC are unable to

control any of the cameras and cannot view historic footage. Staff within this area maybe employees of GWRC, Transdev or Armourguard. Access to the SCC is restricted to authorised personnel, except with written permission from the Transdev Security Manager.

GWRC have a console to access footage located at the Walter Street office. There are only two GWRC staff who have user accounts to enable access. The console is located within an open plan office within a corner to minimise shoulder surfing potential. The console is generally only utilised when there are reduced staff numbers within the office to further reduce this risk. All GWRC staff and contractors who have access to the open plan area of the office are bound by confidentiality clauses as part of their contracts.

The Transdev and Armourguard contracts detail that staff must only disclose information / footage for the purposes requested by GWRC as specified within Security Management Plan. This plan currently doesn't provide details of any allowable disclosures.

If an individual wants to receive a copy of their information / footage they can request this by email or through the Metlink or GWRC Service Centre. Generally, people are directed to contact the Police if the footage relates to a crime. Frontline staff don't currently have any documentation regarding how to handle privacy requests. They generally email them to the Privacy Officer if they are unsure.

Privacy requests are logged in accordance with GWRC standard process and the Privacy Officer is responsible for dealing with the request. Where footage exists but is not able to be released due to issues with de-identifying others contained within the footage, a written record of the incident may be made available instead. This process is detailed in the Public Transport Group Camera Surveillance Policy. To date there have been very few requests for footage from individuals.

In the event of some unlawful activity being recorded on GWRC's surveillance cameras anywhere in the rail network Transdev may pass that footage of the incident over to Police for investigation. This disclosure is detailed in the current and new privacy statements. When footage is shared with Police none of the identities of the people contained within the footage are masked.

There is an agreement in place between Transdev and NZ Police signed on the 11 July 2017. In accordance with this agreement Transdev will provide Police with access to the RMC where pertinent significant matters arise, and timeliness is a factor. This access allows them to view live footage from the stations and surrounding areas. The agreement also allows for Police to make requests to Transdev for footage across the rail network without a production order. This footage will be used to contribute to crime prevention, crime and other investigations and / or resolutions. These disclosures are detailed in the current and new privacy statements.

Requests by Police for footage are usually made by email to the Transdev Security Manager. If requests are made by phone, due to the urgency of the situation, the process for extracting footage will commence, however the footage will not be provided to Police until the request has been received in writing. There is a log kept of requests received by Transdev and this is available for GWRC review on request. Currently there are approximately three requests received per day from Police.

Once the required footage requested by the Police has been identified it is downloaded by the Transdev Security Manager and burnt to CD which is then couriered to Police. When footage is shared with Police none of the identities of the people contained within the footage are masked.

GWRC have approved KiwiRail Train Control to have access to the live and previous thirty minutes footage from the stations and surrounding areas. None of the identities of the people contained within the footage are masked. KiwiRail use the footage for the purposes of Wellington Network Situational Awareness, and ultimately improved decision making around the prioritisation and

efficient operation of the rail network within Wellington. Train Control Instruction A033 details how KiwiRail staff may use the footage. There is currently no formal written agreement authorising this disclosure and details of the disclosure are not included within the Privacy Statement.

For all requests for footage by Transdev employees a CCTV Access Request Form must be completed and returned to the Transdev Security Manager. These requests may be made in the circumstances such as complaints from customers, investigations into staff or to assist with details of operations. The usage is possibly not in accordance with the purposes the information was collected for. It is at the discretion of the Transdev Security Manager if these requests are responded to and GWRC is not proactively informed.

There is an agreement, dated March 2011, in place between KiwiRail and the Rail and Maritime Transport Union (RMTU). This agreement requires the Transdev Security Manager to advise the RMTU of any requests for footage that include Transdev staff and provide details of the staff involved. The RMTU Representative has the right to view any footage prior to release. They require that KiwiRail must obtain permission from all other parties in the footage prior to making it available for viewing. Normally the RMTU Representative does not request a viewing of the footage. Details of this disclosure are not included within the Privacy Statement.

If an individual wants to receive a copy of their footage collected using a bodyworn camera they can request this through Transdev. GWRC is not able to provide this footage. There is some likelihood that multiple requests will be received by GWRC in error. These requests will be transferred to Transdev. However detailed standard operating procedures do not exist detailing how this transfer will occur.

4.4 Security of Personal Information

Red Wolf are contracted to manage the camera surveillance system infrastructure and software for the station cameras. Transdev are contracted to manage the security of the on train camera system.

There is not currently a security risk assessment for either system. There are also no details available about ongoing security control testing and maintenance activities.

4.5 Retention and Disposal of Personal Information

Each station also has their own server which holds approximately fourteen days footage. It is overwritten automatically once the storage reaches capacity with the oldest footage being overwritten first.

The onboard train footage is saved for approximately fourteen days on each train. The exact retention period for each train depends on the number of hours the individual train is utilised for. If the drives are removed from a train to download the footage, then the drives are wiped post the download. The drives are then returned to another train.

In the event footage is downloaded or copies made then the footage may be kept for up to a year unless it is required to be held longer for use in legal proceedings. The Transdev Security Manager is responsible for managing all downloaded and copied footage. There are currently no documented procedures available about how downloaded or copied footage is handled.

The system audit logs are retained for an unknown period and then overwritten when the storage reaches capacity.

4.6 Unique Identifiers

No unique identifiers are assigned as part of this solution.

4.7 Risk Assessment

The key risks to GWRC associated with usage of camera surveillance on the rail network are as follows. These have been evaluated based on the GWRC Risk Management Policy 2013.

Ref	Description	IPP	Existing controls	Inherent			Recommended mitigations	Residual		
				Likelihood	Consequence	Rating		Likelihood	Consequence	Rating
A01	More personal information is collected than required as part of the footage.	1	<ul style="list-style-type: none"> Limited areas of collection. Monitoring of Surveillance Officer behaviour. No audio recording. Regular checks on area of collection. Surveillance Officer training. 	Unlikely	Moderate	Medium	<ul style="list-style-type: none"> AA16 - Standard operating procedures. 	Highly Unlikely	Moderate	Low
A02	More personal information is collected than required regarding staff usage of the system.	1	<ul style="list-style-type: none"> Data minimisation. 	Highly Unlikely	Moderate	Low		Highly Unlikely	Moderate	Low
A03	Individuals are unaware of why their information is being collected and who will get the information.	3	<ul style="list-style-type: none"> Privacy statement available from Service Centre. Privacy statement on Metlink website. Questions answered by Service Centre. Signage at stations. Signage on trains. Six monthly review of signage. Terms of Carriage. Visible cameras. 	Almost Certain	Moderate	High	<ul style="list-style-type: none"> AA01 - Additional signage in Wellington station. AA02 - Additional signage on trains AA14 - Service Centre training. AA18 - Updated privacy statement. AA19 – Bodyworn camera information. 	Unlikely	Single	Low
A04	Staff are unaware of why their information is being collected and who will get the information.	3	<ul style="list-style-type: none"> Public Transport Group Camera Surveillance Policy. 	Almost Certain	Single	Medium	<ul style="list-style-type: none"> AA06 - Communication of updated Public Transport Group Camera Surveillance Policy. AA11 - Privacy statement on system. AA15 - Signage in ticket offices and RMC. 	Highly Unlikely	Individual	Low
A05	Individuals feel the collection is unreasonably intrusive.	4	<ul style="list-style-type: none"> Limited areas of collection. No audio recording. Privacy statement on Metlink website. Questions answered by Service Centre. Signage at stations. Signage on trains. Terms of Carriage. Visible cameras. 	Likely	Moderate	Medium	<ul style="list-style-type: none"> AA01 - Additional signage in Wellington station. AA02 - Additional signage on trains AA14 - Service Centre training. AA15 - Signage in ticket offices and RMC. AA18 - Updated privacy statement. AA19 – Bodyworn camera information. 	Unlikely	Single	Low

Ref	Description	IPP	Existing controls	Inherent			Recommended mitigations	Residual		
				Likelihood	Consequence	Rating		Likelihood	Consequence	Rating
A06	A security breach causes unauthorised access to footage or system logs.	5	<ul style="list-style-type: none"> Red Wolf contract. Transdev contract. 	Likely	Major	High	<ul style="list-style-type: none"> AA10 - Penetration testing. AA12 - Regular security control validation. AA13 - Security risk assessment. AA17 - System updates. 	Highly Unlikely	Moderate	Low
A07	An individual's request for a copy of their information / footage is not actioned.	6	<ul style="list-style-type: none"> Centrally logged. Established process for handling requests. Public Transport Group Camera Surveillance Policy. 	Almost Certain	Individual	Medium	<ul style="list-style-type: none"> AA06 - Communication of updated Public Transport Group Camera Surveillance Policy. AA14 - Service Centre training. AA19 – Bodyworn camera information. 	Rare	Individual	Low
A08	Information disclosed to a third party e.g. Police, is incorrect	8	<ul style="list-style-type: none"> Daily checks on system performance. Red Wolf contract. Time syncing. 	Rare	Moderate	Low		Rare	Moderate	Low
A09	Information is held longer than required.	9	<ul style="list-style-type: none"> Automated overwrite capabilities. Retention schedule documented for footage. 	Likely	Moderate	Medium	<ul style="list-style-type: none"> AA07 – Decide, document and implement log retention schedule. AA16 – Standard operating procedures. 	Highly Unlikely	Single	Low
A10	Footage or log information is used for other purposes.	10	<ul style="list-style-type: none"> Approval process. Monitoring of system logs. Public Transport Group Camera Surveillance Policy. Red Wolf contract. Restricted download abilities. Security Management Plan. Transdev contract. 	Highly Unlikely	Moderate	Low	<ul style="list-style-type: none"> AA06 – Communication of updated Public Transport Group Camera Surveillance Policy. AA09 – Masking of individuals. 	Highly Unlikely	Moderate	Low
A11	Footage or log information is disclosed to more staff than required.	11	<ul style="list-style-type: none"> GWRC employment contract. Kiwirail contract. Location of console. Monitoring of system logs. Public Transport Group Camera Surveillance Policy. Restricted access to RMC and SCC. Security Management Plan. Times of console. Trandev contract. 	Highly Unlikely	Moderate	Low	<ul style="list-style-type: none"> AA06 – Communication of updated Public Transport Group Camera Surveillance Policy. AA09 – Masking of individuals. 	Rare	Moderate	Low

Ref	Description	IPP	Existing controls	Inherent			Recommended mitigations	Residual		
				Likelihood	Consequence	Rating		Likelihood	Consequence	Rating
A12	Footage is proactively disclosed to Police without due cause.	11	<ul style="list-style-type: none"> Experienced staff. Licensed staff. Monitoring of system logs. Public Transport Group Camera Surveillance Policy. Restricted download abilities. Security Management Plan. 	Highly Unlikely	Single	Low	<ul style="list-style-type: none"> AA06 – Communication of updated Public Transport Group Camera Surveillance Policy. 	Highly Unlikely	Single	Low
A13	Footage is disclosed to Police on request without production order.	11	<ul style="list-style-type: none"> Privacy statement on Metlink website. Public Transport Group Camera Surveillance Policy. 	Almost Certain	Moderate	High	<ul style="list-style-type: none"> AA05 – Change to parties to the Letter of Agreement with NZ Police. 	Highly Unlikely	Moderate	Low
A14	Footage is disclosed to Transdev employees for purposes other than which it was collected.	11		Almost Certain	Moderate	High	<ul style="list-style-type: none"> AA04 – Change to business process for requests. AA09 – Masking of individuals. AA18 – Updated privacy statement. 	Highly Unlikely	Single	Low
A15	Footage details are disclosed to the RMTU without the individuals consent.	11		Almost Certain	Moderate	High	<ul style="list-style-type: none"> AA03 – Cancellation of agreement with RMTU. AA04 – Change to business process for requests. 	Rare	Individual	Low
A16	Footage details are disclosed to the KiwiRail Train Control without authorisation.	11	<ul style="list-style-type: none"> Email agreement with GWRC for sharing. 	Almost Certain	Moderate	High	<ul style="list-style-type: none"> AA08 – Formal agreement with KiwiRail. AA09 – Masking of individuals. AA18 – Updated privacy statement. 	Rare	Individual	Low
A17	Red Wolf, Transdev or Armourguard disclose information to an unauthorised party.	11	<ul style="list-style-type: none"> Armourguard contract. Licensed staff. Monitoring of system logs. Public Transport Group Camera Surveillance Policy. Red Wolf contract. Restricted download abilities. Transdev contract. 	Highly Unlikely	Moderate	Low	<ul style="list-style-type: none"> AA06 – Communication of updated Public Transport Group Camera Surveillance Policy. AA09 – Masking of individuals. 	Rare	Moderate	Low
A18	GWRC discloses information to an unauthorised party.	11	<ul style="list-style-type: none"> GWRC employment contract. Monitoring of system logs. Public Transport Group Camera Surveillance Policy. 	Highly Unlikely	Moderate	Low	<ul style="list-style-type: none"> AA06 – Communication of updated Public Transport Group Camera Surveillance Policy. AA09 – Masking of individuals. 	Rare	Moderate	Low
A19	An individual contained within footage who is not the person of interest is included in disclosed footage.	11	<ul style="list-style-type: none"> Manual masking for privacy requests. 	Almost Certain	Single	Medium	<ul style="list-style-type: none"> AA09 – Masking of individuals. 	Rare	Single	Low

4.8 Action Plan

The following actions are agreed in relation to the camera surveillance in use on the rail network.

Ref	Agreed action	Related risks	Who is responsible	Completion date
AA01	Install additional signage inside Wellington Station and ensure it is clearly visible.	A03 A05	Barry Fryer	August 2018
AA02	Install additional signage on the trains and ensure it is visible from anywhere on the train.	A03 A05	Barry Fryer	August 2018
AA03	Advise Transdev GWRC no longer wish for details of footage to be shared with the RMTU.	A15	Barry Fryer	August 2018
AA04	Update the business process for requests to ensure: <ul style="list-style-type: none"> • Only pre-approved scenarios are approved by the Transdev Security Manager. • Authorisation is received from the Responsible Officer for non-approved scenarios. • Footage is only used for the same purpose it was collected for. • RMTU are not advised of all requests. 	A14 A15	Barry Fryer	August 2018
AA05	Change the parties to the Letter of Agreement with NZ Police for provision of footage without a production order.	A13	Barry Fryer	August 2018
AA06	Communication of updated Public Transport Group Camera Surveillance Policy to all staff with access to the system once agreed.	A04 A07 A10 A11 A12 A17 A18	Paul Kos	July 2018
AA07	Decide, document and implement retention schedule for how long logs pertaining to system usage should be held.	A09	Barry Fryer	July 2018
AA08	Develop a Memorandum of Understanding with KiwiRail for provision of footage. Once signed update the privacy statements.	A16	Barry Fryer	August 2018
AA09	Explore options to mask the identity of individuals unless they need to be explicitly identified.	A10 A11 A14 A16 A17 A18	IT	December 2018

Ref	Agreed action	Related risks	Who is responsible	Completion date
AA10	Complete network security penetration testing and address any issues identified.	A06	IT	August 2018
AA11	Develop a privacy statement that is available to users of the system when they login.	A04	Privacy Officer	August 2018
AA12	Develop a regular programme of IT security control validation.	A06	IT	December 2018
AA13	Complete a security risk assessment and update this PIA to reflect any risks that may impact on the privacy of personal information.	A06	IT	August 2018
AA14	Provide training for staff within the Metlink Call Centre / GWRC Service Centre on: <ul style="list-style-type: none"> The new privacy statement. How to handle requests from individuals for access. How to handle requests from Police for access. 	A03 A05 A07	Privacy Officer	August 2018
AA15	Install signage in the RMC and ticket offices advising camera surveillance is operational.	A04 A05	Barry Fryer	July 2018
AA16	Develop standard operating procedures to include: <ul style="list-style-type: none"> Accessing live footage. Accessing historic footage. Handling requests from individuals for access. Handling requests from Police for access. Copying footage. Disposing of footage. 	A01 A09	Barry Fryer	August 2018
AA17	Complete all required system updates to ensure that the latest version of software and security patches are installed.	A06	Red Wolf	August 2018
AA18	Update the privacy statement including the camera surveillance page on the GWRC and Metlink websites once signed off.	A03 A05 A14 A16	Sally Parker	August 2018
AA19	Clarification provided to Transdev that they are the operator of the bodyworn cameras and as such need to provide information to the public in accordance with the Privacy Act.	A03 A05 A07	Barry Fryer	July 2018

5 Bus Services

5.1 Collection of Personal Information

There is a requirement in the PTOM contract for all Bus Operators to ensure that all vehicles are fitted with a camera surveillance system which is visible to customers. The camera surveillance system and all footage collected is owned and operated by the relevant Bus Operator.

The minimum number of cameras required by GWRC is detailed in the following table. However, the Bus Operator may choose to install more cameras if they wish.

Location	Small Vehicle (SV)	Medium Vehicle (MV)	Large Vehicle (LV)	Double Decker (DD)
Entrance platform and passenger / driver interface	✓	✓	✓	✓
Rear of interior seated area looking forwards covering rear seated area	✓	✓	✓	✓
Exit area providing the driver with an unobstructed view of rear door		✓	✓	✓
Between the rear door and the front door of the vehicle. Mounted either at the front looking rearwards or at the rear door looking forwards and covering the wheelchair space		✓	✓	✓
Rear of the upper saloon area looking forwards covering rear seated areas				✓
Top of the stairwell directed down the stairwell				✓
Front of upper saloon looking rearwards				✓
Facing forward to road ahead of vehicle	✓	✓	✓	✓
Kerb side facing towards the rear monitoring door activity	✓	✓	✓	✓

GWRC have requested that the camera footage must commence a maximum of three minutes after the vehicle has been started and must continue until at least fifteen minutes after the vehicle is turned off. GWRC require that footage must be collected in all light conditions and suggest some cameras should have infrared capabilities to enable this requirement to be met.

GWRC have requested a microphone be installed near the drivers cab to record audible sounds, conversations and other activities that occur within two metres of the driving seat upon activation of the duress alarm. GWRC require that no audio recording is to be made unless the duress alarm is activated.

GWRC have requested that footage is collected for the purposes of:

- Collecting evidence for prosecution of criminal events
- Investigation of incidents

- Ensuring Farebox Revenue is appropriately collected.

However, the Bus Operator may also choose to collect footage for other reasons at their discretion. The capturing of footage is also used to deter criminal events, objectionable behaviours and safety incidents occurring.

The Bus Operator is responsible for ensuring individuals are made aware that camera surveillance is in operation upon the bus and that they operate the system. GWRC have identified several potential locations within the bus where signage could be included. Due to the requirement that the signage indicates the collection purpose and the system operator the signs cannot be developed by GWRC in isolation.

The PTOM contract requires each Bus Operator to develop a privacy statement that covers the camera surveillance operations. GWRC can provide feedback on the privacy statements. Currently several the privacy statements are still under development or will need to be updated to include the details of the camera surveillance system. GWRC require that the Bus Operator make the privacy statement freely available upon request by any person. Currently not all the Bus Operators have their privacy statement publicly available.

The GWRC privacy statement is currently being updated and will replace the existing Metlink privacy statement (<https://www.metlink.org.nz/privacy/>) as well as the current GWRC Customer Privacy Policy (<http://www.gw.govt.nz/privacy-statement/>) which do not mention the use of camera surveillance on buses explicitly. The new privacy statement details that camera surveillance is in operation and directs individuals to a webpage detailing the locations where surveillance is used. This webpage details that the camera surveillance on the buses is not operated by GWRC and directs the individual to the relevant Bus Operator's privacy statement.

If an individual contacts either the Metlink Call Centre or the GWRC Service Centre regarding the on bus camera surveillance they will need to be directed to the relevant Bus Operator. Currently Service Centre staff have no documented process for dealing with these requests.

5.2 Use of Personal Information

The use of the footage collected is determined by the relevant Bus Operator. However, GWRC have requested access so they can use the footage for:

- Investigation of incidents
- Ensuring Farebox Revenue is appropriately collected.

Within the driver's cab there is a monitor where the driver can view any or all of the images in real time. The intent is that this is utilised by the driver for passenger safety reasons. However, each individual Bus Operator will individually determine how they wish their drivers to utilise this functionality.

GWRC do not require the cameras on the buses to be actively monitored. However, they do require that a maintenance check is completed at least every six months by the Bus Operator and that the footage is easily and readily downloadable.

5.3 Disclosure of Personal Information

If an individual wants to receive a copy of their footage they can request this through the relevant Bus Operator. GWRC is not able to provide this footage. There is some likelihood that multiple requests will be received by GWRC in error. These requests will be transferred to the relevant Bus

Operator. However detailed standard operating procedures do not exist detailing how this transfer will occur.

The PTOM contract requires that GWRC have access to footage for the purposes of auditing the Bus Operator's compliance with the contract. The contract also allows GWRC to request images and recordings where they relate to an incident or where GWRC wishes to ensure Farebox revenue is appropriately collected. There are currently no standard operating procedures in place between GWRC and the Bus Operators to enable this activity.

Information received by GWRC from a Bus Operator must not be shared with any other party including the Police. Any further disclosure of the footage collected is determined by the relevant Bus Operator. GWRC do require that any disclosure be in accordance with the Privacy Act.

5.4 Security of Personal Information

The Bus Operator is ultimately responsible for the security of the footage. GWRC requires that the Bus Operator takes all reasonable steps to ensure that the footage is protected against misuse, loss, unauthorised access, modification or disclosure. They are also required to ensure only authorised and required personnel have access to the footage.

In the event of a security breach of the footage the Bus Operator is required to notify GWRC.

5.5 Retention and Disposal of Personal Information

GWRC require that all footage is kept for a minimum of fourteen days. After this GWRC has consented for the information to be overwritten. As the Bus Operator owns and operates the system it is their choice how long they wish to keep the footage for over and above fourteen days and how it is disposed of. The Bus Operator is required to comply with the Privacy Act which requires they don't retain information for longer than it is required.

Any footage received by GWRC from a Bus Operator must only be held as long as required. There are currently no standard operating procedures detailing how footage received from a Bus Operator should be handled.

5.6 Unique Identifiers

No unique identifiers will be assigned by GWRC as part of this solution.

5.7 Risk Assessment

The key risks to GWRC associated with usage of camera surveillance on the buses are as follows. These have been evaluated based on the GWRC Risk Management Policy 2013.

Ref	Description	IPP	Existing controls	Inherent			Recommended mitigations	Residual		
				Likelihood	Consequence	Rating		Likelihood	Consequence	Rating
B01	Individuals are unaware of why their information is being collected, by who and who will get the information and believe GWRC are responsible.	3	<ul style="list-style-type: none"> Privacy statement on Metlink website. Questions answered by Service Centre. Terms of Carriage. Visible cameras. 	Almost Certain	Single	Medium	<ul style="list-style-type: none"> BA01 - Bus Operators privacy statements. BA02 - GWRC review of Bus Operator privacy statements. BA03 - Service Centre training. BA04 - Signage on the bus. BA06 - Updated GWRC privacy statement. 	Unlikely	Single	Low
B02	Individuals feel the collection is unreasonably intrusive.	4	<ul style="list-style-type: none"> Limited audio recording. Privacy statement on Metlink website. Questions answered by Service Centre. Terms of Carriage. Visible cameras. 	Likely	Single	Medium	<ul style="list-style-type: none"> BA01 - Bus Operators privacy statements. BA03 - Service Centre training. BA04 - Signage on the bus. BA06 - Updated GWRC privacy statement. 	Unlikely	Single	Low
B03	A security breach causes unauthorised access to footage and the public opinion is that GWRC are responsible.	5	<ul style="list-style-type: none"> Contract with Bus Operator. Requirement to notify of breach. 	Highly Unlikely	Single	Low	<ul style="list-style-type: none"> BA04 - Signage on the bus. BA06 - Updated GWRC privacy statement. 	Highly Unlikely	Single	Low
B04	An individual's request for a copy of their footage is sent to GWRC in error.	6	<ul style="list-style-type: none"> Established process for handling requests. 	Almost Certain	Individual	Medium	<ul style="list-style-type: none"> BA01 - Bus Operators privacy statement. BA02 - GWRC review of Bus Operator privacy statements. BA03 - Service Centre training. BA04 - Signage on the bus. BA05 - Standard operating procedures. BA06 - Updated GWRC privacy statement. 	Almost Certain	Individual	Medium
B05	Footage provided to GWRC by a Bus Operator is held longer than required.	9	<ul style="list-style-type: none"> GWRC Privacy Policy. 	Likely	Moderate	Medium	<ul style="list-style-type: none"> BA05 - Standard operating procedures. 	Highly Unlikely	Single	Low
B06	Footage provided to GWRC by a Bus Operator is used for an unapproved purpose.	10	<ul style="list-style-type: none"> Approval process. GWRC Privacy Policy. 	Unlikely	Moderate	Medium	<ul style="list-style-type: none"> BA05 - Standard operating procedures. 	Highly Unlikely	Moderate	Low
B07	Footage provide to GWRC by a Bus Operator is disclosed to a third party.	11	<ul style="list-style-type: none"> Experienced staff. GWRC Privacy Policy. 	Likely	Moderate	Medium	<ul style="list-style-type: none"> BA05 - Standard operating procedures. 	Highly Unlikely	Moderate	Low

Ref	Description	IPP	Existing controls	Inherent			Recommended mitigations	Residual		
				Likelihood	Consequence	Rating		Likelihood	Consequence	Rating
B08	Individuals make privacy complaints to GWRC in error.	All	<ul style="list-style-type: none"> Established process for handling complaints. 	Likely	Individual	Low	<ul style="list-style-type: none"> BA01 - Bus Operators privacy statement. BA02 - GWRC review of Bus Operator privacy statements. BA03 - Service Centre training. BA04 - Signage on the bus. BA06 - Updated GWRC privacy statement. 	Highly Unlikely	Individual	Low

5.8 Action Plan

The following actions are agreed in relation to the camera surveillance in use on the buses.

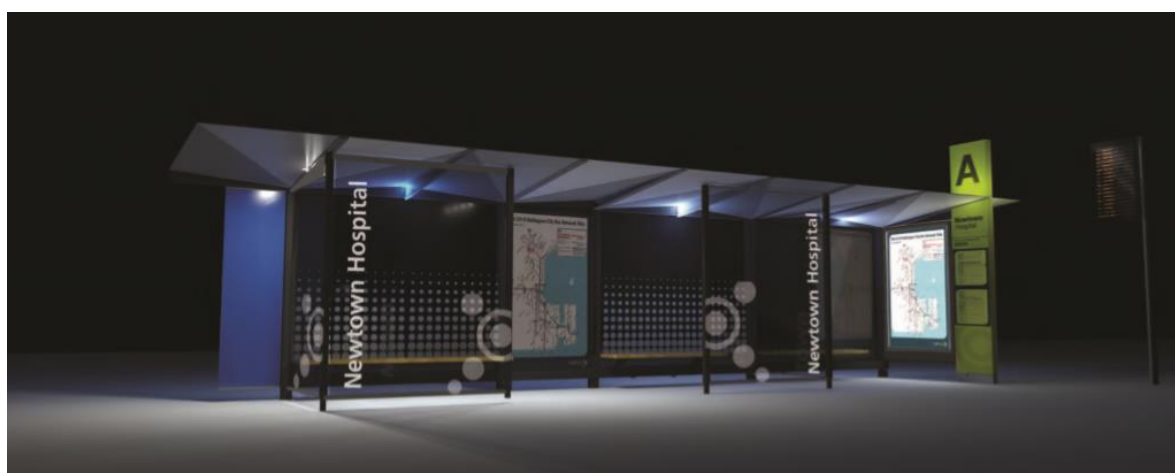
Ref	Agreed action	Related risks	Who is responsible	Completion date
BA01	Ensure each Bus Operator has a privacy statement and that it is publicly available, ideally on their website.	B01 B02 B04 B08	Rhona Hewitt	Pre Go Live
BA02	Review each Bus Operator's privacy statement and ensure that it adequately covers the details of the camera surveillance in operation, how to request access and how to make a complaint.	B01 B04 B08	Rhona Hewitt	Pre Go Live
BA03	Provide training for staff in the Service Centre on: <ul style="list-style-type: none"> • The arrangements for the buses around the camera surveillance and GWRC's role. • How to handle requests from individuals for access to footage onboard buses • How to handle requests from Police for access to footage from onboard buses • How to handle privacy complaints from individuals relating to the buses. 	B01 B02 B04 B08	Rhona Hewitt	Pre Go Live
BA04	Work with the Bus Operators to develop signage for inside the buses and ensure it is visible from anywhere where footage is collected.	B01 B02 B03 B04 B08	Rhona Hewitt	Pre Go Live
BA05	Develop standard operating procedures to include: <ul style="list-style-type: none"> • Requesting footage. • Transferring access requests. • Transferring privacy complaints. • Approved uses of footage. • Disposing of footage. 	B04 B05 B06 B07	Rhona Hewitt	Pre Go Live
BA06	Update the GWRC privacy statement including the camera surveillance page on the GWRC and Metlink websites once signed off.	B01 B02 B03 B04 B08	Sally Parker	August 2018

6 Bus Hubs

6.1 Collection of Personal Information

Each bus shelter located at a Bus Hub has a camera installed at each end under the canopy and are clearly visible. The cameras only record visual footage and can work in very low light conditions. The cameras cover the area inside the bus shelter as well as a small area outside of the bus shelter which is captured either through clear line of sight or through the transparent screens of the shelter. The cameras operate 24 hours a day, seven days a week.

Except for the Bus Hub at the bus exchange at Wellington Station the cameras are owned by GWRC and operated on GWRC's behalf by Red Wolf. The cameras at the bus exchange are owned and operated by Wellington City Council and are therefore outside of the scope of this PIA.



The Public Transport Group Camera Surveillance Policy details that footage is to only be collected for the purposes of:

- Immediately detecting criminal events, objectionable behaviours and safety incidents
- Collecting evidence for prosecution of criminal events
- Collecting information of asset condition and damage
- Monitoring of patterns of travel behaviour in groups of customers where no individual customer is uniquely identifiable.

The capturing of footage is also used to deter criminal events, objectionable behaviours and safety incidents occurring.



Individuals are made aware that camera surveillance is in operation for the purposes of crime prevention and safety through the inclusion of signage both inside the bus shelter and on the outside. This signage is currently under development but will be similar to other Metlink camera operating signs. The signs will be visible to any person prior to entering the area being captured as part of the footage. The signs contain both the phone number for Metlink and the website address.

The GWRC privacy statement is currently being updated and will replace the existing Metlink privacy statement

(<https://www.metlink.org.nz/privacy/>) as well as the current GWRC

Customer Privacy Policy (<http://www.gw.govt.nz/privacy-statement/>) which do not mention the use of camera surveillance at the Bus Hubs explicitly.

The new privacy statement is currently in the process of being reviewed by ELT and is expected to be in place within the next month. The new privacy statement details that camera surveillance is in operation and directs individuals to a page detailing the locations where surveillance is used and the purposes. This includes details of the camera surveillance at the Bus Hubs.

If an individual contacts either the Metlink or GWRC Service Centre they are provided details regarding the usage of camera surveillance based on the information contained within the updated privacy statement or can request a copy of the privacy statement.

The Conditions of Carriage also detail that camera surveillance is in operation and directs individuals to the GWRC privacy statement for further information.

Limited personal information is also collected about the actions of GWRC and Red Wolf employees who access the camera surveillance system for administrative reasons. The information collected relates to the individual who logged on to the system and the actions they took. This is contained within the logs of the system. The staff are not made aware at the time that their behaviours are being monitored.

6.2 Use of Personal Information

The cameras at the Bus Hubs are not actively monitored. However, a maintenance check is completed twice a day by Red Wolf for the primary purpose of maintenance of the system and the bus shelter assets. Red Wolf employees and two GWRC employees have access to the footage through specially provided consoles.

The Public Transport Group Camera Surveillance Policy details that footage can only be used for the purpose for which it was collected. Camera footage obtained from the Bus Hubs must only be downloaded in response to an incident / request.

The footage may also only be used, with the prior approval of the Responsible Officer, for the following related purposes:

- Inquiries relating to the investigation of other criminal offences or safety incidents
- Training of security staff and maintenance of the system
- Research, such as into the nature of security incidents, patterns in use or travel behaviour, or evaluation of the operation of particular camera systems.

The Red Wolf contract details that Red Wolf must only use footage for the purposes requested by GWRC as specified within the Standard Operating Procedures (SOPs). Currently the SOPs have not been developed.

Information collected within the system logs regarding the usage of the system by Red Wolf and GWRC staff is used to identify unauthorised behaviours and to investigate any incidents.

Audits are planned to be undertaken of the records of who accesses the system, copies footage and provides images to external parties.

6.3 Disclosure of Personal Information

Any individual who is recorded by the cameras at the Bus Hubs has the right to access that footage. Red Wolf and GWRC employees also have the right to a copy of the personal information held about them in the system logs.

If an individual wants to receive a copy of their information / footage they can request this by email or through the Metlink or GWRC Service Centre. Frontline staff don't currently have any documentation regarding how to handle privacy requests.

Privacy requests are logged in accordance with GWRC standard process and the Privacy Officer is responsible for dealing with the request. Where footage exists but is not able to be released due to issues with de-identifying others contained within the footage, a written record of the incident may be made available instead. This process is detailed in the Public Transport Group Camera Surveillance Policy. It is expected that the level of privacy requests relating to the Bus Hubs will be similar to the current level for rail services, which is a few a year.

Any requests for footage taken at the bus exchange at Wellington Station are transferred to Wellington City Council.

In the event of unlawful activity being carried out and footage being available relating to the incident then GWRC or Red Wolf, as authorised by GWRC, may pass the related footage to the Police for investigation.

If the Police believe that unlawful activities have been captured on the footage, then they may request GWRC provide the footage to help their investigation. It is expected that the level of requests relating to the Bus Hubs will be similar to those for rail services which is currently approximately three a day. There is currently no Memorandum of Understanding in place to allow sharing of footage other than with a production order.

Any release of footage to third parties other than Police and insurance companies must be approved by the Responsible Officer. The process for handling these requests for Bus Hub footage has not yet been defined.

The Red Wolf contract details that Red Wolf must only disclose information / footage for the purposes requested by GWRC as specified within the Standard Operating Procedures (SOPs). Currently the SOPs have not been developed.

If any other third party wishes to receive a copy of the footage then this must be approved by the General Manager, Public Transport.

The identity of individuals within the footage is not masked when visible to staff using a console. All Red Wolf Operators are licenced under the Private Security Personnel and Private Investigators Act 2010. Red Wolf only have access from a control room which is locked and has restricted access.

GWRC will have a console to access footage. There will only be two staff with user accounts for access. As the console is located within an open plan office it will be located within a corner to minimise shoulder surfing potential. The console will generally only be utilised when there are reduced staff numbers within the office. All GWRC staff and contractors who have access to the open plan area of the office are bound by confidentiality clauses as part of their contracts.

6.4 Security of Personal Information

A security risk assessment for the camera surveillance system operating at the Bus Hubs is currently underway. This PIA will be updated to reflect the outcomes of this work once available.

6.5 Retention and Disposal of Personal Information

Camera footage from the Bus Hubs will be retained for fourteen days and then overwritten. Any copies of footage will be kept for up to a year unless it is required to be held longer for use in legal proceedings.

Red Wolf are contractually required to audit the system to ensure the disposal schedule is being followed.

The system audit logs are retained for an unknown period and then overwritten when the storage reaches capacity.

6.6 Unique Identifiers

No unique identifiers are assigned as part of this solution.

6.7 Risk Assessment

The key risks to GWRC associated with usage of camera surveillance at the Bus Hubs are as follows. These have been evaluated based on the GWRC Risk Management Policy 2013.

Ref	Description	IPP	Existing controls	Inherent			Recommended mitigations	Residual		
				Likelihood	Consequence	Rating		Likelihood	Consequence	Rating
C01	More personal information is collected than required as part of the footage.	1	<ul style="list-style-type: none"> Limited areas of collection. No audio recording. Regular checks on area of collection. 	Highly Unlikely	Moderate	Low		Highly Unlikely	Moderate	Low
C02	More personal information is collected than required regarding staff usage of the system.	1	<ul style="list-style-type: none"> Data minimisation. 	Highly Unlikely	Moderate	Low		Highly Unlikely	Moderate	Low
C03	Individuals are unaware of why their information is being collected and who will get the information.	3	<ul style="list-style-type: none"> Privacy statement available from Service Centre. Privacy statement on Metlink website. Questions answered by Service Centre. Terms of Carriage. Visible cameras. 	Almost Certain	Moderate	High	<ul style="list-style-type: none"> CA08 - Service Centre training. CA09 - Signage inside the bus shelter. CA10 - Signage outside the bus shelter. CA12 - Updated privacy statement. 	Unlikely	Single	Low
C04	Staff are unaware of why their information is being collected and who will get the information.	3	<ul style="list-style-type: none"> Public Transport Group Camera Surveillance Policy. 	Almost Certain	Single	Medium	<ul style="list-style-type: none"> CA01 - Communication of updated Public Transport Group Camera Surveillance Policy. CA04 - Privacy statement on system. 	Highly Unlikely	Individual	Low
C05	Individuals feel the collection is unreasonably intrusive.	4	<ul style="list-style-type: none"> Limited areas of collection. No audio recording. No private property captured without permission. Privacy statement on Metlink website. Questions answered by Service Centre. Terms of Carriage. Visible cameras. 	Likely	Moderate	Medium	<ul style="list-style-type: none"> CA08 - Service Centre training. CA09 - Signage inside the bus shelter. CA10 - Signage outside the bus shelter. CA12 - Updated privacy statement. 	Unlikely	Single	Low
C06	A security breach causes unauthorised access to footage or system logs.	5	<ul style="list-style-type: none"> Liquid IT contract. Liquid IT requirements. Red Wolf contract. 	Unlikely	Moderate	Medium	<ul style="list-style-type: none"> CA05 - Penetration testing. CA07 - Security risk assessment. 	Highly Unlikely	Moderate	Low
C07	An individual's request for a copy of their information / footage is not actioned.	6	<ul style="list-style-type: none"> Centrally logged. Established process for handling requests. Public Transport Group Camera Surveillance Policy. 	Almost Certain	Individual	Medium	<ul style="list-style-type: none"> CA01 - Communication of updated Public Transport Group Camera Surveillance Policy. CA08 - Service Centre training. 	Rare	Individual	Low

Ref	Description	IPP	Existing controls	Inherent			Recommended mitigations	Residual		
				Likelihood	Consequence	Rating		Likelihood	Consequence	Rating
C08	Information disclosed to a third party e.g. Police, is incorrect	8	<ul style="list-style-type: none"> Daily checks on system performance. Time syncing. 	Rare	Moderate	Low		Rare	Moderate	Low
C09	Information is held longer than required.	9	<ul style="list-style-type: none"> Retention schedule documented for footage. 	Likely	Moderate	Medium	<ul style="list-style-type: none"> CA02 - Decide, document and implement log retention schedule. CA11 - Standard operating procedures. 	Highly Unlikely	Single	Low
C10	Footage or log information is used for other purposes.	10	<ul style="list-style-type: none"> Approval process. Public Transport Group Camera Surveillance Policy. Red Wolf contract. System logs. 	Likely	Moderate	Medium	<ul style="list-style-type: none"> CA01 - Communication of updated Public Transport Group Camera Surveillance Policy. CA04 - Monitoring of system logs. CA11 - Standard operating procedures. CA13 - Masking of individuals. 	Highly Unlikely	Moderate	Low
C11	Footage or log information is disclosed to more staff than required.	11	<ul style="list-style-type: none"> GWRC employment contract. Location of console. Public Transport Group Camera Surveillance Policy. Red Wolf contract. System logs. Usage times of console. 	Highly Unlikely	Moderate	Low	<ul style="list-style-type: none"> CA01 - Communication of updated Public Transport Group Camera Surveillance Policy. CA04 - Monitoring of system logs. CA11 - Standard operating procedures. CA13 - Masking of individuals. 	Rare	Moderate	Low
C12	Footage is proactively disclosed to Police without due cause.	11	<ul style="list-style-type: none"> Experienced staff. Licensed staff. Public Transport Group Camera Surveillance Policy. System logs. 	Unlikely	Single	Low	<ul style="list-style-type: none"> CA01 - Communication of updated Public Transport Group Camera Surveillance Policy. CA04 - Monitoring of system logs. CA11 - Standard operating procedures. 	Highly Unlikely	Single	Low
C13	Footage is disclosed to Police on request without production order.	11		Almost Certain	Moderate	High	<ul style="list-style-type: none"> CA04 - Monitoring of system logs. CA11 - Standard operating procedures. CA03 - Memorandum of Understanding with NZ Police and update to privacy statements. 	Highly Unlikely	Moderate	Low
C14	Red Wolf discloses information to an unauthorised party.	11	<ul style="list-style-type: none"> Licensed staff. Public Transport Group Camera Surveillance Policy. Red Wolf contract. System logs. 	Highly Unlikely	Moderate	Low	<ul style="list-style-type: none"> CA01 - Communication of updated Public Transport Group Camera Surveillance Policy. CA04 - Monitoring of system logs. CA13 - Masking of individuals. 	Rare	Moderate	Low

Ref	Description	IPP	Existing controls	Inherent			Recommended mitigations	Residual		
				Likelihood	Consequence	Rating		Likelihood	Consequence	Rating
C15	GWRC discloses information to an unauthorised party.	11	<ul style="list-style-type: none"> GWRC employment contract. Public Transport Group Camera Surveillance Policy. System logs. 	Highly Unlikely	Moderate	Low	<ul style="list-style-type: none"> CA01 - Communication of updated Public Transport Group Camera Surveillance Policy. CA04 - Monitoring of system logs. CA13 - Masking of individuals. 	Rare	Moderate	Low
C16	An individual contained within footage who is not the person of interest is included in disclosed footage.	11	<ul style="list-style-type: none"> Manual masking for privacy requests. 	Almost Certain	Single	Medium	<ul style="list-style-type: none"> CA13 - Masking of individuals. 	Rare	Single	Low

6.8 Action Plan

The following actions are agreed in relation to the camera surveillance in use at the Bus Hubs.

Ref	Agreed action	Related risks	Who is responsible	Completion date
CA01	Communication of updated Public Transport Group Camera Surveillance Policy to all staff with access to the system once agreed.	C04 C07 C10 C11 C12 C14 C15	Paul Kos	Pre Go Live
CA02	Decide, document and implement retention schedule for how long logs pertaining to system usage should be held.	C08 C09	Rhona Hewitt	Pre Go Live
CA03	Develop a Memorandum of Understanding with NZ Police for provision of footage without a production order. Once signed update the privacy statements.	C13	Rhona Hewitt	August 2018
CA04	Develop a monitoring programme for the system logs to identify unauthorised behaviours.	C10 C11 C12 C13 C14 C15	Paul Kos	August 2018
CA05	Complete penetration testing and address any issues identified.	C06	Stuart MacDonald	Pre Go Live
CA06	Develop a privacy statement for the system to advise users of collection of logs.	C04	Privacy Officer	Pre Go Live
CA07	Complete the scheduled security risk assessment and update this PIA to reflect any risks that may impact on the privacy of personal information.	C06	Stuart MacDonald	Pre Go Live
CA08	Provide training for the Service Centre on: <ul style="list-style-type: none"> The new privacy statement. How to handle requests from individuals for access. How to handle requests from Police for access. 	C03 C05 C07	Privacy Officer	Pre Go Live
CA09	Develop signage for inside the bus shelter and ensure it is visible from anywhere in the shelter.	C03 C05	David Boyd	Pre Go Live

Ref	Agreed action	Related risks	Who is responsible	Completion date
CA10	Develop signage for outside the bus shelter and ensure it is visible from anywhere where footage is collected.	C03 C05	David Boyd	Pre Go Live
CA11	Develop standard operating procedures to include: <ul style="list-style-type: none"> • Accessing live footage. • Accessing historic footage. • Handling live incidents. • Reporting incidents to the Police. • Handling requests from individuals for access. • Handling requests from Police for access. • Copying footage. • Disposing of footage. • Ongoing audit of usage. 	C09 C10 C11 C12 C13	Rhona Hewitt	Pre Go Live
CA12	Update the privacy statement including the camera surveillance page on the GWRC and Metlink websites once signed off.	C03 C05	Privacy Officer	Pre Go Live
CA13	Explore options to mask the identity of individuals unless they need to be explicitly identified.	C10 C11 C14 C15 C16	IT	December 2018

7 Authorisation

The Business Owner is ultimately responsible for ensuring that the Privacy Impact Assessment has the appropriate scope, and that the recommendations are actioned.

Authorised by	Signature	Date
Wayne Hastie General Manager Public Transport Group		

Forward a copy of the signed document to [GWRC's Privacy Officer](#).