Queensland Government Enterprise Architecture

Public Wi-Fi guideline

Guideline on Queensland Government provision of public Wi-Fi network services

Final

December 2015

V1.0.0

PUBLIC

Document details

|  |  |
| --- | --- |
| 1. **Security classification**
 | 1. PUBLIC
 |
| 1. **Date of review of security classification**
 | 1. December 2015
 |
| 1. **Authority**
 | 1. Queensland Government Chief Information Officer
 |
| 1. **Author**
 | 1. Queensland Government Chief Information Office
 |
| 1. **Documentation status**
 |  | 1. Working draft
 |  | 1. Consultation release
 | 1. 🗹
 | 1. Final version
 |

Contact for enquiries and proposed changes

All enquiries regarding this document should be directed in the first instance to:

Queensland Government Chief Information Office
qgea@digital.qld.gov.au

Acknowledgements

This version of the *Public Wi-Fi guideline* was developed and updated by Queensland Government Chief Information Office, in consultation with the Information and Technology Partners, Department of Agriculture and Fisheries.

Feedback was also received from a number of agencies, which was greatly appreciated.

Copyright

*Public Wi-Fi guideline*

Copyright © The State of Queensland (Department of Science, Information Technology and Innovation) 2015

Licence



This work is licensed under a Creative Commons Attribution 4.0 International licence. To view the terms of this licence, visit <http://creativecommons.org/licenses/by/4.0/>. For permissions beyond the scope of this licence, contact qgcio@qgcio.qld.gov.au.

To attribute this material, cite the Queensland Government Chief Information Office.

Information security

This document has been security classified using the Queensland Government Information Security Classification Framework (QGISCF) as PUBLIC and will be managed according to the requirements of the QGISCF.

Contents

[1 Introduction 4](#_Toc431365532)

[1.1 Purpose 4](#_Toc431365533)

[1.2 Audience 4](#_Toc431365534)

[1.3 Scope 4](#_Toc431365535)

[2 Relationship to Use of ICT facilities and devices (IS38) 4](#_Toc431365536)

[2.1 Defining ‘users’ 5](#_Toc431365537)

[3 Internet service provision 5](#_Toc431365538)

[3.1 Using an external internet service provider 5](#_Toc431365539)

[4 Setting up the service 6](#_Toc431365540)

[4.1 Service configuration 6](#_Toc431365541)

[4.2 Service quality 8](#_Toc431365542)

[4.3 Security risks 8](#_Toc431365543)

[4.4 Privacy 9](#_Toc431365544)

[4.5 User obligations and rights 9](#_Toc431365545)

[4.6 Content filtering/bandwidth allocation and throttling 10](#_Toc431365546)

[4.7 Monitoring 10](#_Toc431365547)

[4.8 Location of services 11](#_Toc431365548)

[5 Use of the service 11](#_Toc431365549)

[5.1 Authorised use 11](#_Toc431365550)

[5.2 Unauthorised use 11](#_Toc431365551)

[5.3 Infringement of conditions 11](#_Toc431365552)

[5.4 Conditions of use 12](#_Toc431365553)

[6 Terms and conditions checklist 12](#_Toc431365554)

[6.1 Service quality 12](#_Toc431365555)

[6.2 Security 12](#_Toc431365556)

[6.3 Privacy 13](#_Toc431365557)

[6.4 User obligation and rights 13](#_Toc431365558)

[6.5 Content filtering/bandwidth and throttling 13](#_Toc431365559)

[6.6 Monitoring 13](#_Toc431365560)

[6.7 Unauthorised use 14](#_Toc431365561)

[6.8 Termination of use 14](#_Toc431365562)

[6.9 Release and indemnity 14](#_Toc431365563)

# Introduction

## Purpose

A Queensland Government Enterprise Architecture (QGEA) guideline provides information for Queensland Government departments on the recommended practices for a given topic area. Guidelines are for information only and departments are not required to comply. They are intended to help departments understand the appropriate approach to addressing a particular issue or undertaking a particular task.

Queensland Government departments may choose to provide users with a public Wi-Fi service for authorised use. This guideline has been developed to assist departments with the provision of public Wi-Fi services including guidance on service configuration and developing the terms and conditions of use

## Audience

##### This document is primarily intended for

* chief executive officers/other senior officers who authorise the provision of public Wi-Fi services,
* human resource professionals, and
* information management/ICT policy staff.

## Scope

### In scope

This guideline provides advice to Queensland Government departments on the provision of a public Wi-Fi network by outlining the key considerations with respect to service configuration and terms and conditions of use of government-provided public Wi-Fi.

### Out of scope

1. Employee use of non-government provided Wi-Fi networks with government issued mobile devices.
2. Detailed technical advice on the infrastructure to be used in setting up government-provided Wi-Fi networks.

# Relationship to Use of ICT services, facilities and devices (IS38)

The [Use of ICT services, facilities and devices policy (IS38)](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/use-of-ict-services-facilities-and-devices-policy-is38) was primarily created to cover employee use, however, as per the [IS38 implementation guideline](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/use-of-ict-services-facilities-and-devices-implementation-guideline), departments should clearly state which employees are covered under their policy, for example, students, volunteers, work experience, or other external bodies authorised by an departments to use government-provided [ICT services, facilities and devices](https://www.forgov.qld.gov.au/news-events-and-consultation/glossary). As such, many of the principles and requirements from IS38 can still be applied to [employees](https://www.forgov.qld.gov.au/news-events-and-consultation/glossary) and other users of Wi-Fi services.

For example:

* such provision still needs to be determined by an department’s chief executive officers
* terms of use need to be clearly articulated to users prior to acceptance of the service
* users should have a clear understanding of what monitoring may take place when using these services
* users need to be aware of and acknowledge the government policy on any restrictions and consequences of misuse in the terms and conditions prior to using ICT services, facilities and devices.

## Defining ‘users’

For the purpose of this guideline, the term ‘users’ will be used to define the various types of users that the department provides the service to.

Users can be classified as either identified, authenticated or anonymous. Identified users are those that have provided an identity (e.g. – Username, email address, etc.). Authenticated users have also provided authentication that they are the owner of the provided identity (e.g. - Passphrase, token etc. associated with that identity). Anonymous users are not identified.

Users can range from employees to guest users that require temporary internet access for specific locations or events (e.g. training rooms and workshops), to the general public.

When dealing with users beyond employees, there arises some difference in the types of consequences that can be applied when dealing with misuse. As such, it is important to understand the risks of providing access to these services in a fair and equitable manner, while also implementing controls to minimise inappropriate use of these publicly funded services.

# Internet service provision

## Using an external internet service provider

By using an external ISP for the provision of a public Wi-Fi service, departments may lose some control over how their network is operated and will be subject to the internet service provider’s (ISP) terms and conditions unless thoroughly reviewed at the contract and support negotiation stage. Prior to signing any service agreement, departments should ensure that the following aspects are covered in the service terms:

1. Resiliency

The ISP has the capacity and appropriate incident response provisions in place to respond to events that may impact on service performance (e.g. attack, high traffic levels, rate limiting, etc.).

1. Priority of service provision

The ISP places a high priority on Queensland Government departments requiring support.

1. Service availability

The ISP can guarantee an acceptable level of service availability and has an appropriate service continuity plan.

1. Traffic monitoring reports

The ISP will provide the reports in a suitable format type and an appropriate frequency.

Additional information on QITC specifications regarding internet services are contained in *Module 13* located on the [QITC website](https://www.forgov.qld.gov.au/finance-and-procurement/procurement/buy-for-queensland-government/buying-categories/ict-products-and-services/about-the-qitc-framework).

# Setting up the service

## Service configuration

### Key considerations

Departments should take into account the following configuration questions prior to setting up a public Wi-Fi network.

1. **Will the service be available to anyone?**

The service can be made available to some or all types of users depending on departmental requirements. Regardless of the scope of users, departments should define who is considered an authorised user of the network in the terms and conditions.

1. **Will the service be available at all times?**

The public Wi-Fi network should be accessible at all times, although a temporary (guest) Wi-Fi network can be set up for a specific areas or events (e.g. training rooms, workshops, etc.).

1. **Will the service be fully automated?**

Connecting to the public Wi-Fi network should be quick and simple for users. There are certain steps that are necessary to connect to the network (e.g. enabling wireless adapter, opening the list of available wireless networks, selecting the desired network, etc.), however the number of additional steps should be kept to a minimum.

1. **Will the public Wi-Fi be purchased ‘as-a-service’ or not?**

If a department wishes to outsource both the provision and operation of the public Wi-Fi network to an ISP, an as-a-service model could be used. However, if a department wishes to provide and operate the Wi-Fi network in-house, the service would not be purchased ‘as-a-service’. Internet access would be supplied by an ISP and the department would then manage the operation of the network internally. Refer to the [ICT-as-a-service Decision Framework](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/ict-as-a-service-decision-framework-overview) for further guidance on the appropriate delivery model to use.

1. **Will Australian Communications and Media Authority (ACMA) regulations apply?**

The ACMA may direct an ISP or carriage service provider (CSP) to comply with a particular code if they believe that the ISP or CSP is not already doing so. Failure to comply with such direction may amount to an offence under the relevant Act.

1. **Will a special telecommunications licence be required?**

The owner of a network unit (cable or wireless facility) which is used to supply carriage services (e.g. telephony or internet) to the public, must hold a carrier licence. However, CSP’s providing carriage services including internet access services are not required to obtain a telecommunications licence from ACMA.

For more information regarding CSP obligations, see ACMA’s [Know Your Obligations](http://www.acma.gov.au/~/media/Broadband%20Applications%20and%20Services/Publication/pdf/Know%20Your%20Telecommunications%20Industry%20Obligations%20Booklet.pdf) booklet.

1. **Will users need to obtain an account?**

A public Wi-Fi network can be provided without the need for account creation. For example, the Victorian Government’s free public Wi-Fi network does not require details such as emails, passwords or other personal data to be provided in order to use the network. However, any new solutions or systems provided by Queensland Government departments and Queensland Government ICT service providers that require client registration and/or client identification must use the Queensland Government client identity management (CIDM) system in accordance with the [Client identity management policy](https://www.qgcio.qld.gov.au/products/qgea-documents/3250-client-identity-management-policy). The [Client identity management policy](https://www.qgcio.qld.gov.au/products/qgea-documents/3250-client-identity-management-policy) defines a consistent implementation approach to ensure that departments move towards full adoption of the Queensland Government CIDM system

Minimising the number of steps and the amount of information required to register and access the service will help improve the customer experience and reduce administrative tasks if the network is managed internally.

1. **Will network access duration be limited?**

Restricting the duration of network access by timed session or through generic access codes/passwords is a practical way of limiting the number of users accessing the network and can also help minimise extended use or the high consumption of bandwidth that typically contributes to poor network performance. Using generic access codes for network access does not involve the collection of personal information, therefore no privacy issues exist. If a department wishes to use a user-specific password, there would be the collection and use of the individual’s personal information so the information privacy principles within the [Information Privacy Act 2009 (Qld)](https://www.legislation.qld.gov.au/ACTS_SLs/Acts_SL_I.htm) would apply.

1. **Letting users know what they can expect from the service?**

Information regarding service provision obligations or user expectations should be specified in the terms and conditions of service use. Refer to 4.2 Service quality below for further information.

1. **What type of access do they get (e.g. quality, speed, security, privacy etc.)?**

Refer to 4.2 Service quality below for further guidance. All information regarding service access should be outlined in the terms and conditions.

1. **Are there any costs incurred by the users? If so, do these need to be communicated to users before signing up? Will refunds be given?**

If a department wishes to charge users for use of the public Wi-Fi service, it is recommended that expert advice is sought regarding billing, refunds and PCI-DSS compliance (credit card information handling). For further guidance, please refer to the following resources:

* ‘Billing’ section in Module 13 Internet Services located the [QITC website](https://www.forgov.qld.gov.au/finance-and-procurement/procurement/buy-for-queensland-government/buying-categories/ict-products-and-services/about-the-qitc-framework)
* PCI Data Security Standard (PCI DSS) [website](https://www.pcisecuritystandards.org/security_standards/)
1. **Will the department offer help and support to users?**

Departments should provide users with clear and simple instructions on how to connect to and disconnect from the Wi-Fi network with some basic troubleshooting instructions. However, a department is not obliged to provide detailed technical support, particularly if the service is managed by an external ISP.

1. **Will a Wi-Fi survey be conducted?**

A Wi-Fi network site survey can be an effective way to assess the environment in order to design and configure the Wi-Fi network in a way that minimises interference and optimises efficiency and performance. There are a range of services available that provide tools such as Wi-Fi planning, site survey and mapping and frequency spectrum analysis to achieve these outcomes.

1. **Will testing/ongoing quality checks be conducted?**

Departments should conduct sufficient testing of their Wi-Fi network prior to deployment to ensure that the service is operating as required. Ongoing checks are also suggested to ensure that that the service quality is maintained to the service level stated in the terms and conditions.

In addition to the advice provided above, further deliberation should be undertaken to ensure all department-specific requirements are identified and considered, particularly with respect to the following questions as they will have a direct impact on the infrastructure and service configuration required to effectively deliver the service.

* How many concurrent users is the service catering for (e.g. 10, 100, 1000)?
* What sort of features are required (e.g. will a dedicated hotspot gateway be required or is a guest network sufficient)?
* Where will users be able to access the service (e.g. only in a specific building/s and/or in open space hotspots)?

## Service quality

### Information quality

Departments providing the public Wi-Fi network cannot guarantee the quality of the information that users may access on the internet. As such departments may wish to provide a statement that users are responsible for determining the validity, quality and relevance of any information obtained whilst using the Wi-Fi network.

### Speed, download limit and reliability

Departments should provide Wi-Fi internet access at a limited download speed that balances the number of concurrent users and sufficient connectivity speeds. For example, Brisbane City Council provides free Wi-Fi access at a maximum download speed of 512kbps which effectively balances the usage amongst all users. It is important to note that user’s accessing the network via a virtual private network (VPN) may experience lower network speeds.

The download limit set for the network should also balance time and data usage so that users can adequately consume authorised web content for the duration of the session (i.e. daily or by timed session).

A department should make their best effort to ensure stable and secure access to the network for users, however there is no guarantee that the service will remain free of errors, interception or interference. Similarly, a department should make their best effort to rectify any identified network issues, however a department is not obliged to do so within any specified time frame.

## Security risks

It is recommended that departments conduct a risk assessment prior to setting up a public

Wi-Fi network to address any security risks that may be identified. Some of the topics or risks that should be considered in the risk assessment include:

* unauthorised use
* malware
* interception by third parties
* privacy
* encryption
* reputation (of Queensland Government).

A department can request that users accept or agree to the terms and conditions of service use in order to access the network. This is an effective way to create a contractual relationship with the users in order to mitigate the risk of unauthorised use. Normally this process would involve the collection and use of the individual’s personal information, therefore the information privacy principles within the [Information Privacy Act 2009 (Qld)](https://www.legislation.qld.gov.au/ACTS_SLs/Acts_SL_I.htm) would apply. However, through the Queensland Government CIDM system, only verified identity information will be offered as an identity attribute and as such no privacy issues would exist. For further information on specific authentication requirements, refer to the [CIDM standard](https://www.qgcio.qld.gov.au/products/qgea-documents/3251-client-identity-management-standard?lnk=QS0yLTMyNTEtMQ).

Once the public Wi-Fi network is operational, departments should monitor and assess activity over the Wi-Fi network to manage the risks identified. Refer to 4.7 Monitoringfor more information regarding network monitoring.

Departments must also ensure that users are aware that they are responsible for their own protection when using Wi-Fi services, including:

* the sites or online services that they are accessing or content they are downloading
* ensuring that firewall and virus protection software is installed, enabled and up-to-date
* ensuring that usernames, passwords and personal information are kept private.

## Privacy

If a department collects ‘personal information’ in its provisioning of public Wi-Fi, it should ensure compliance with the privacy obligations in the *Information Privacy Act 2009.* However, it is also the responsibility of the users of the public Wi-Fi network to ensure that their privacy is safeguarded against other users of the Wi-Fi network. For more information regarding privacy and user obligations for public Wi-Fi hotspots, please refer to the [Office of the Information Commissioner](https://www.oic.qld.gov.au/guidelines/for-community-members/Information-sheets-privacy-principles/privacy-and-using-public-wi-fi-hotspots) website.

Departments can collect [metadata](https://www.qgcio.qld.gov.au/products/glossary) (e.g. activity logs of users including the MAC and IP addresses of connected devices) if the addresses collected aren’t linked to individuals as this does not constitute personal information. The activity logs collected must be retained for a minimum of 7 years after the last action in accordance with Section 13.2.3 of the [General Retention and Disposal Schedule for Administrative Records](http://www.archives.qld.gov.au/Recordkeeping/RetentionDisposal/Pages/GRDS.aspx) (QDAN 249 v.7)*.*

## User obligations and rights

There are a number of requirements that users would need to satisfy in order to access public Wi-Fi services, such as:

* possessing suitable computing equipment with wireless LAN capability (i.e. IEEE 802.11b, 802.11g or 802.11n)
* the associated software is installed and configured for use with the service (i.e. device drivers and internet browsers)
* users’ device has its own power source.

Terms and conditions of service use should be clearly displayed (i.e. upon login and on a web page about the service) so that users are aware of, understand and acknowledge their responsibilities and policy obligations when using government-provided [ICT services, facilities and devices](https://www.forgov.qld.gov.au/news-events-and-consultation/glossary). Users must also acknowledge the terms and conditions of service use (e.g. clicking an ‘agree’ button or ticking an ‘accept’ box) prior to gaining access to the wireless service. As part of the terms and conditions of service use, users should not have the right to resell this service to a third party.

## Content filtering/bandwidth allocation and throttling

A department can reserve the right to filter the traffic on the public Wi-Fi network at all times. Departments can also limit or throttle bandwidth to certain services and websites to prevent the abuse of the service through excessive use.

If traffic filtering and/or bandwidth restrictions is being conducted, this should be clearly communicated to users as part of the terms and conditions of use.

A potential risk of filtering traffic is unintentionally denying users access to certain sites or content being used for appropriate purposes, however it is still suggested that filtering traffic be applied to minimise any unauthorised use. Departments can either restrict access to authorised sites only or block certain sites containing unlawful, criminal, offensive or obscene material as outlined in *Section 2* of the [Authorised and unauthorised use guideline](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/authorised-and-unauthorised-use-of-ict-services-facilities-and-devices-guideline)*.*

For example, Queensland Rail applies content filtering to the following items/conditions:

1. Only HTTP, HTTPS and email traffic will be allowed
2. FTP, VPN and Peer to Peer traffic will not be transported
3. Web access to unauthorised material (unlawful, criminal, offensive or obscene) as outlined in Section 2.2 of the [Authorised and unauthorised use guideline](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/authorised-and-unauthorised-use-of-ict-services-facilities-and-devices-guideline) will be filtered.

## Monitoring

Departments should have a clear idea of what information they wish to monitor and how it feeds back into the business. An agency can monitor what is on a user’s device if the user is visiting unencrypted sites, although if the user is accessing a secure site (i.e. HTTPS) or is using a VPN to browse sites, the service provider will only be able to see that the user has visited the site but will not be able to obtain or read any content (e.g. on visited sites or within emails) that could be used to identify the user.

A department at the least will have a record of all activity over the Wi-Fi network largely in the form of [metadata](https://www.forgov.qld.gov.au/news-events-and-consultation/glossary). The metadata may include the following information:

* MAC address of the user’s device
* IP address
* sites visited and time spent there
* download amounts
* user’s type of device
* operating system of user’s device
* internet browser used.

Monitoring the traffic will also assist the service provider in detecting any unauthorised use of the service. Although depending on the level of monitoring undertaken, the retention of users’ activity logs may be considered ‘public records’ and if so would be subject to the *Public Records Act 2002* and the [General Retention and Disposal Schedule for Administrative Records](http://www.archives.qld.gov.au/Recordkeeping/RetentionDisposal/Pages/GRDS.aspx)*.* Subsequently, it is suggested that departments seek advice from QSA regarding the management of these records. Further, if an ISP is used to provide the public Wi-Fi service, under the [Telecommunications (Interception and Access) Act 1979](https://www.comlaw.gov.au/Series/C2004A02124)*,* telecommunication’s service providers are required to retain and secure telecommunications data (not content) for two years.

## Location of services

### Wi-Fi coverage overlaps

In the instance that multiple departments are located in close proximity to each other (e.g. on the same floor), departments should ensure that they liaise with other departments when setting up a public Wi-Fi network/s so that any overlap or network interference in minimised. A combined Wi-Fi service may be considered as an appropriate option.

### User responsibility

Users connected to a public Wi-Fi network are likely to be using the service in close proximity to each other. As a result, individual users of the service have a responsibility to be mindful of their use of the service in order to respect the peace, privacy and personal space of others around them.

# Use of the service

## Authorised use

Refer to *Section 2.1* of the [Authorised and unauthorised use guideline](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/authorised-and-unauthorised-use-of-ict-services-facilities-and-devices-guideline) for detailed information on the authorised use of government-provided ICT services, facilities and devices.

## Unauthorised use

Refer to *Section 2.2* of the [Authorised and unauthorised use guideline](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/authorised-and-unauthorised-use-of-ict-services-facilities-and-devices-guideline)for detailed information on the unauthorised use of government-provided ICT services, facilities and devices. Information regarding unauthorised use should be considered by all departments.

## Infringement of conditions

### Termination of use

Departments can reserve the right to suspend a user’s session if:

* the maximum session time has elapsed
* there is a belief that the use of the service is excessive (e.g. consuming the maximum daily download limit in an unreasonable period of time)
* the service is being used for unauthorised use (i.e. unlawful, criminal, offensive or obscene)
* there is a breach of any of the stated terms and conditions
* users are reselling the service to a third party
* the wireless connection to the network that the user is accessing is lost, disconnected or becomes out of range
* no activity is detected from the user’s wireless enabled device for a certain period of time (e.g. 30 mins) while connected to the network.

In the instance that the service is terminated for any of the reasons outlined above, there should be a message displayed to advise the user as to why their service has been terminated.

## Conditions of use

### Release and indemnity

As part of the terms and conditions of which users agree to or accept, departments should consider including a release and discharge clause to ensure that the Queensland Government is not liable for any loss or damages that users sustain from the use of the public Wi-Fi service except in the event that departments breach users’ privacy. The clause should also state that departments will report any criminal activities identified to the appropriate authorities.

### Terms and conditions

The information contained in 4 Setting up the service and 5 Use of the servicecan form part of the terms and conditions for government-provided public Wi-Fi services. However, when developing the terms and conditions, agencies should also take into consideration department-specific requirements and other public Wi-Fi terms and conditions, such as:

* Brisbane City Council
<http://www.brisbane.qld.gov.au/facilities-recreation/parks-venues/parks/park-facilities/wi-fi-parks/wi-fi-parks-terms-conditions>
* AdelaideFree Wi-Fi network by Internode
<http://www.internode.on.net/pdf/legal/internode-hotspot-end-user-terms.pdf>
* City of London Wi-Fi Network
<http://www.thecloud.net/free-wifi/uk-wlan-terms-and-conditions/>

Departments can use splash screens to display the terms and conditions and other information (e.g. educative or informative on the department’s services). Apart from the information regarding the terms and conditions that the user (unidentified) agrees to, splash screens do no collect individual’s information, therefore no privacy issues arise from their use.

# Terms and conditions checklist

## Service quality

* Departments cannot guarantee the quality of the information that user’s access on the internet.
* Departments should provide Wi-Fi access at a limited download speed (e.g. 512kbps) that balances the number of concurrent users and sufficient connectivity speeds.
* The download limit set for the network should also balance time and data usage.
* Departments cannot guarantee that the service will remain free from errors, interception or interference.
* Departments should make their best effort to ensure stable and secure access to the network for users and rectify any identified network issues.

See [4.2 Service quality](#_Service_quality) for further information.

## Security

* A department can require users to accept or agree to the terms and conditions of service use in order to access the network.
* Once the public Wi-Fi network is operational, departments should monitor and assess activity over the Wi-Fi network to manage the risks identified.
* Departments must also ensure that users are aware that they are responsible for their own protection when using Wi-Fi services

See [4.3 Security risks](#_Security_risks) for further information.

## Privacy

* If a department collects ‘personal information’ in its provisioning of public Wi-Fi, it should ensure compliance with the privacy obligations in the *Information Privacy Act 2009.*
* It is the responsibility of the users of the public Wi-Fi network to ensure that their privacy is safeguarded against other users of the Wi-Fi network.

See [4.4 Privacy](#_Privacy) for further information.

## User obligation and rights

* Users need to satisfy a number of requirements in order to access public Wi-Fi services, such as possessing suitable computing equipment with own power source and having associated software installed and configured.
* Terms and conditions of service use should be clearly displayed so that users are aware of, understand and acknowledge their responsibilities and policy obligations when using government provided ICT services, facilities and devices.
* Users must acknowledge the terms and conditions of service use prior to gaining access to the wireless service.
* Users should not have the right to resell this service to a third party.

See [4.5 User obligations and rights](#_User_obligations_and) for further information.

## Content filtering/bandwidth and throttling

* A department can reserve the right to filter the traffic on the public Wi-Fi network at all times, however this should be clearly communicated to users as part of the terms and conditions of use.

See [4.6 Content filtering/bandwidth allocation and throttling](#_Content_filtering/bandwidth_allocat) for further information.

## Monitoring

* A department can monitor what is on a user’s device if the user is visiting unencrypted sites, although if the user is accessing a secure site (i.e. HTTPS) or is using a Virtual Private Network (VPN) to browse sites, the service provider will only be able to see that the user has visited the site but will not be able to obtain or read any content (e.g. on visited sites or within emails) that could be used to identify the user.
* A department at the least will have a record of all activity over the Wi-Fi network largely in the form of metadata.
* Depending on the level of monitoring undertaken, the retention of users’ activity logs may be considered ‘public records’ and if so would be subject to the *Public Records Act 2002* and the [General Retention and Disposal Schedule for Administrative Records](http://www.archives.qld.gov.au/Recordkeeping/RetentionDisposal/Pages/GRDS.aspx).
* If an ISP is used to provide the public Wi-Fi service, under the *Telecommunications (Interception and Access) Act 1979*, telecommunication’s service providers are required to retain and secure telecommunications data (not content) for two years.

See [4.7 Monitoring](#_Monitoring) for further information.

## Unauthorised use

* Refer to Section 2.2 of the [Authorised and unauthorised use guideline](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/authorised-and-unauthorised-use-of-ict-services-facilities-and-devices-guideline) for detailed information on the unauthorised use of government-provided ICT services, facilities and devices.

See [5 Use of the service](#_Use_of_the) for further information.

## Termination of use

Departments can reserve the right to suspend a user’s session if:

* the maximum session time has elapsed
* there is a belief that the use of the service is excessive (e.g. consuming the maximum daily download limit in an unreasonable period of time)
* the service is being used for unauthorised use (i.e. unlawful, criminal, offensive or obscene)
* there is a breach of any of the stated terms and conditions
* users are reselling the service to a third party
* the wireless connection to the network that the user is accessing is lost, disconnected or becomes out of range
* no activity is detected from the user’s wireless enabled device for a certain period of time (e.g. 30 mins) while connected to the network.

See [5 Use of the service](#_Use_of_the) for further information.

## Release and indemnity

* Departments should consider including a release and discharge clause to ensure that the Queensland Government is not liable for any loss or damages that users sustain from the use of the public Wi-Fi service except in the event that the department breaches users’ privacy. The clause should also state that departments will report any criminal activities identified to the appropriate authorities.

See [5 Use of the service](#_Use_of_the) for further information.