

Queensland Worker Screening Services Privacy Policy

1. About this policy

1.1. Purpose

Queensland Worker Screening Services (QWSS), part of the Department of Justice (DoJ), is committed to protecting the privacy of individuals and ensuring that personal information is handled in accordance with the *Information Privacy Act 2009* (Qld) (IP Act).

The IP Act requires us to have a Privacy Policy which outlines the way we handle personal information.

This Privacy Policy applies to all our officers and meets our obligations under 'Queensland Privacy Principle 1 - Open and transparent management of personal information'. The Office of the Information Commissioner has published a [guide to the QPPs](#).

In this document 'your information' means your personal information and sensitive information.

This Policy is to be read together with [Department of Justice Privacy Policy](#).

2. Our functions and responsibilities

QWSS manage two distinct screening programs:

1. Blue Card Services (BCS): This program administers the Working with Children Check (WWCC) under the blue card system, which operates under the [Working with Children Check Act 2000](#) (WWCC Act).
2. Disability Worker Screening (DWS): This program administers the National Disability Insurance Scheme (NDIS) Worker Screening and Queensland Disability Worker Screening Checks, under the [Disability Services Act 2006](#) (DS Act).

BCS and DWS assess whether individuals are eligible to work with children or people with disability, based on a range of assessable information. We also monitor for any new information that might impact an individual's eligibility to continue this work. Additionally, we monitor organisations and individuals' compliance with their obligations outlined in the WWCC and DS Acts (the Acts).

We collect, consider, hold and share relevant personal and sensitive information, including sharing information between BCS and DWS to exercise functions and powers, and meet our responsibilities, under our legislation.

3. What is personal information?

The IP Act defines personal information as information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion, whether the information or opinion is true or whether the information or opinion is recorded in a material form.

Personal information can also be 'protected information' under the WWCC and DS Acts. Protected information refers to a range of information obtained about you, if applicable, to inform a risk assessment.

This can include the following information about a person:

- Police and related information
- Domestic violence
- Disciplinary information
- Adverse interstate working with children check information
- Information disclosed by the NDIS Quality and Safeguards Commission (NDIS Commission), an NDIS worker screening unit or other prescribed entity

- Information about a person's mental health, for example information about a proceeding in the Mental Health Court or the Mental Health Review Tribunal
- NDIS disciplinary or misconduct information, and
- Other information that the chief executive has considered in making an employment-screening decision about the person.

4. What is sensitive information?

Under Schedule 5 of the IP Act, sensitive information for an individual means:

- racial or ethnic origin
- political opinions
- membership of a political association
- religious beliefs or affiliations
- philosophical beliefs
- membership of a professional or trade association
- membership of a trade union
- sexual orientation or practices
- criminal record
- health information
- genetic information that is not otherwise health information
- biometric information that is to be used for the purpose of automated biometric verification or
- biometric identification, or
- biometric templates.

5. Personal and sensitive information we collect from you

We aim to limit our collection of your personal and sensitive personal information to only the information we need to carry out our powers, functions, and official duties.

5.1. Information we collect for applications

This may include the following when someone applies for a working with children check or disability worker screening application:

- full legal name, any previous names, title, gender, date of birth, place of birth, current or former professional roles (if applicable)
- sensitive personal information relating to your cultural background (if applicable)
- current contact details including postal, residential and email addresses and phone numbers
- foster or kinship care information, including whether you are applying as a carer or adult household member, and the address at which care is being provided (if applicable)
- teacher registration number or police identification number (if applicable)
- type of child-related work and activity you perform, as well as the details of the organisation the work is performed for (organisation name, contact details) or details of the child-related business your application refers to, including name, contact details and the type of child-related activity to which the business relates

- disability services role and whether you are engaged by a NDIS service provider or funded service provider (if applicable)
- whether you've ever been suspended or refused, barred or excluded from holding a relevant worker screening check in any Australian state or territory
- whether you've been charged, convicted, or found guilty of a criminal offence in Australia or overseas
- whether you've ever had a domestic violence order (including a temporary order), police protection notice or police protection direction made against you by a court or police in Queensland
- whether you've been subject of an investigation by any government agency anywhere in Australia that involved substantiated allegations that you have caused harm to a child in your care (including the removal of a child/children)
- whether you have ever been subject of a workplace misconduct investigation
- previous worker screening clearance card number (if applicable), and
- Queensland Transport and Main Roads (TMR) ID, or TMR customer reference number (e.g. Queensland driver licence number).

If the above personal information is not provided, QWSS may be unable to accept and assess your application.

In addition to specific personal information collected through your application or renewal, QWSS also records anonymous information (voluntary personal information) for statistical purposes.

Please note that as part of the application process you do not have to answer questions about:

- whether you identify as Aboriginal or Torres Strait Islander
- whether you come from a culturally or linguistically diverse background
- whether you are a person with a disability, or
- your education background and qualifications.

Answering these questions is voluntary and any answers provided will not be used in considering your application for a working with children check or disability worker screening clearance.

Your registration and use of the QWSS online application portals involves the collection of your personal information, even if you do not proceed with an application.

QWSS will also obtain relevant information from TMR and Department of Customer Services, Open Data and Small and Family Business (CDSB).

5.2. Information we collect for blue card organisation portal accounts

For persons requesting an account to access the Blue Card Services Organisation Portal (an online system to help employers and volunteer organisations keep track of their records and obligations under the blue card system), we collect the following personal information:

- full legal name, including title and first, middle and last names
- date of birth
- contact telephone numbers
- email address
- blue card number, and
- Queensland Digital Identity (QDI) identifier and username, or alternative identity verification documentation provided to DoJ.

If your personal information is not provided, then DoJ will be unable to accept and assess your application to register as a user of the Organisation Portal.

The Organisation Portal uses cookies to collect anonymous statistical information, including:

- your browser, computer platform and screen resolution
- your traffic patterns through the Organisation Portal, such as:
 - the date and time of your visit
 - the pages and documents accessed
 - the website you visited before ours, and
 - your server address.

QWSS does not identify users or any browser activity outside the Organisation Portal, except in the unlikely event of an investigation, where a law enforcement agency may have a warrant to inspect activity logs.

The Organisation Portal also uses Google Analytics (including display advertising features) and Microsoft Azure to gather anonymous information about users of the Organisation Portal. When you visit the Organisation Portal, your browser automatically sends anonymous information to Google and Microsoft. Examples of the information include the web address of the page that you're visiting, your IP address and demographic information. Google and Microsoft may also use cookies.

We use this data to analyse the pages that are visited, to improve your experience and make sure the Organisation Portal is useful.

5.3. Phone services

When you call Blue Card Services or Disability Worker Screening, we collect personal information to verify your identity, so that we can protect your personal information from unauthorised access or modification by ensuring that we are talking to the right person before disclosing it. This also helps us with your request, to improve our services, train staff, and keep a record of what you share.

We may share your information with relevant agencies as allowed by the IP Act.

If you do not provide the required details, we may not be able to assist you.

5.4. Collection of information for community engagement and other purposes

We collect your contact information for mailing lists, for event registration and surveys. We sometimes use other providers such as Vision6 for bulk mailouts. [Vision6](#) have their own privacy policies.

6. How we use your information and when we give it to others

6.1. Use of information collected for applications

Your personal and sensitive information is used for the following purposes relevant to working with children check or disability worker screening applications:

- to verify your identity
- to enable you to meet your disclosure obligations under the Acts
- to contact you in relation to your application and the blue card system or DWS process
- to send you notices as required by either post, email or SMS, about your application or in relation to the blue card system or DWS process
- to provide notifications regarding application status and upcoming blue/exemption card or DWS renewal requirements
- to assess your application for a blue/exemption card or DWS clearance, or reassess your eligibility to work with children or people with disability
- to enable mandatory consideration of cultural factors as part of the assessment process (if applicable)

- to notify relevant persons, (including your employer; regulatory, governing, disciplinary or supervisory body (if applicable); and NDIS Service providers or funded service providers (if applicable)) regarding the status or outcome of your application, clearance or authority
- to confirm you are currently a Queensland teacher or Queensland police officer (if applicable)
- to display your photograph from the TMR on your blue/exemption card or DWS clearance
- to produce and issue your blue/exemption card or DWS clearance
- to conduct ongoing monitoring of your eligibility to hold a blue/exemption card or DWS clearance
- to administer the blue card and DWS systems
- for record keeping purposes
- to secure access to your information; and
- other matters pertaining to the Acts.

If you choose to answer the voluntary personal questions (refer Section 5.1 above) for an NDIS clearance, this information may be included in the NDIS Worker Screening Database, where it may be accessed by the NDIS Commission. The NDIS Commission will use the information to support policy development and research about NDIS workers and the NDIS, including to help better understand the needs of NDIS workers and reporting statistical information about the NDIS workforce. The NDIS Commission is an independent Commonwealth agency established to improve the quality and safety of NDIS supports and services (for more information about the work of the NDIS Commission see: <https://www.ndiscommission.gov.au/>).

Your information will be de-identified before any other disclosure of it by the NDIS Commission (for example, in any reports produced by the NDIS Commission, or where it is provided to other Commonwealth agencies, such as the National Disability Insurance Agency, to support their policy development and research functions).

6.2. Use of information collected for blue card organisation portal accounts

Your personal information is used for the following purposes relevant to accessing and using the Blue Card Services Organisation Portal:

- verify your identity
- assess your application to become a registered user of the Organisation Portal
- contact you to provide or obtain more information about your application and the Organisation Portal
- complete your registration to use the Organisation Portal
- create your user account
- allow access to and use of the Organisation Portal on behalf of your nominated organisation
- verify your user account at registration
- manage your future logins to the Organisation Portal
- administer the Organisation Portal
- administer the blue card system, including auditing and monitoring compliance with the WWCC Act
- meet your obligations under the WWCC Act, and
- such other purposes as outlined in this privacy notice.

If you use QDI to verify your identity, DoJ will obtain information from QDI to confirm your identity.

6.3. Use of information collected for community engagement and other purposes

Participation in our information session events and surveys help us to better plan and determine customer needs.

7. Giving information to others

7.1. Disclosure of information collected for applications

As part of a working with children check or disability worker screening application, your personal information may also be disclosed to the following persons or organisations for the purposes outlined above and those specified below:

- law enforcement agencies for the purpose of obtaining police information in accordance with the Acts and for general law enforcement purposes, including those purposes set out in the *Australian Crime Commission Act 2002* (Cth)
- courts, tribunals, and other prosecuting authorities for the purpose of assessing your application and ongoing eligibility for an authority/clearance
- prescribed entities, notifiable persons, potential employers and other government agencies in accordance with the Acts
- regulatory, governing, disciplinary or supervisory bodies in accordance with the Acts
- other Australian agencies responsible for screening individuals who work or provide services, or propose to do so, for children and people with disability in accordance with the Acts
- TMR and CDSB to verify identity and arrange for production of the physical card
- third parties which produce the physical card
- universities, other training institutes, recruitment agencies, placement companies and online matching services for the purpose of verifying your DWS application
- if you work or provide services to people with disability, the NDIS Commission for the purpose of being included on the National Worker Screening Database (see paragraph below for more information) or for the NDIS Commission's functions
- if you are providing a child-related home-based care service, your personal information will be published to authorised users of the home-based care register
- confirmation about whether your card is valid
- any other person you have authorised QWSS to discuss your application with
- authorised parties to provide confirmation about whether an authority/clearance is valid in accordance with the Acts, and
- the Queensland Government's information and communication technology service providers for the purpose of system support and development.

7.2. Disclosure to NDIS Worker Screening Database

The NDIS Commission has established and manages the NDIS Worker Screening Database as required by law under the *National Disability Insurance Scheme Act 2013* (Cth).

As part of disability worker screening applications, QWSS will provide the following information to the NDIS Worker Screening Database:

- personal information about a worker that a worker has provided, including in this application form (but not criminal convictions)
- personal information about a worker provided by a worker's NDIS employer, and
- details about clearance decisions undertaken by worker screening units.

The NDIS Worker Screening Database will not include information about any criminal convictions a worker may have, rather it will have the outcomes of worker screening checks.

More information about the NDIS Worker Screening Database can be found at <https://www.ndiscommission.gov.au/>

Once a record has been created for you on the NDIS Worker Screening Database:

- that record will continue to exist on the NDIS Worker Screening Database even if you leave the NDIS sector
- that record may be accessed by NDIS employers who are linked to you and need to check your clearance status. They will be able to see the following about you on the NDIS Worker Screening Database:
 - your worker screening ID
 - date and time your application was created
 - your first and last name
 - gender
 - date of birth
 - State and Country of birth
 - Contact details, including phone and email
 - status (clearance or exclusion)
 - the expiry date of your clearance, and
 - your eligibility to work.

NDIS employers who are linked to you in the NDIS Worker Screening Database will be notified of any changes to your clearance status, for example, if you are no longer cleared to work (such as your clearance being cancelled or replaced with an exclusion). If you cease to be employed by a particular employer, that employer will no longer be linked to you on the NDIS Worker Screening Database and will not be able to access your personal information on the Database.

7.3. Disclosure of information collected for blue card organisation portal accounts

As part of a request to access the Blue Card Organisation Portal, your personal information may also be disclosed to the following persons or organisations for the purposes outlined above and those specified below:

- organisations you work for or provide services to (including other Organisation Portal users)
- DoJ's information and communication technology service providers for the purpose of system support and development, and
- The Queensland Government's 'Tell Us Once' Identity Broker platform.

If you use QDI to verify your identity, QDI will provide information they hold about you to confirm your identity to us.

7.4. Overseas transfer of your information

Your personal information may be transferred overseas in the following circumstances:

- where online services are accessed from outside Australia
- where a service provider who provides services to Queensland Government has servers located outside Australia and, in exceptional circumstances, for card production purposes, and
- where an email service provider stores emails outside Australia, by giving us an email address, you are consenting to the personal information contained within the emails to and from the Queensland Government to be disclosed outside Australia.

8. Where we store your information

8.1. Cloud servers

The department has engaged Microsoft Azure services for integrating information from our web portals to departmental databases.

When you access the online application, data is stored locally on your device during the session. When your application is submitted, the information is sent through the Azure Service Bus temporarily before being sent to our information repository for permanent storage. In some cases, the information may be temporarily stored in Azure Blob storage if the message size exceeds the allowable size limit set by Azure Service Bus. Information is deleted from the Azure services when the transfer to our information repository has been completed.

See the Microsoft Azure Trust Centre for more details. All personal information is protected using the latest encryption techniques, rendering this information unreadable to unauthorised people while housed in the Azure platform.

8.2. On our premises

We store some of our data, including your information on our premises. Where this is the case, we protect your information by imposing a range of security controls like, lockable storage restricted digital access and restricted physical access (such as on restricted access floors of our offices).

9. Quality and security of your information

9.1. Security of your information

We protect the security of personal information we hold from both internal and external threats by:

- regularly assessing the risk of misuse, interference, loss, and unauthorised access, modification, or disclosure your information
- support our officers by providing mandatory and regular targeted privacy and security training to all our business areas
- where appropriate, requiring employees and service providers to sign confidentiality agreements and enter information sharing agreements with us regarding access to, and the use of, personal information held by us or given to service providers
- encouraging our divisions to develop strong local governance frameworks around handling your information,
- frequently reviewing our suite of information management and security policies
- giving our officers clear direction on how to respond to data breaches, in our [Data Breach Notification Policy and Procedure](#)
- implementing the requirements of the Information and Cyber Security Policy which applies to all Queensland government departments ([IS18](#))
- restricting access by our employees, contractors or other authorised parties to your information held by us by role and need for access
- taking unauthorised access to, and use of, personal information seriously, and taking disciplinary action where necessary or warranted
- taking disciplinary or other action on data breaches which may be warranted in those circumstances,
- aiming to securely destroy and identify all your information which we no longer need, and which isn't required under a law for us to keep, and
- undertaking privacy impact assessments on all projects and activities which involve personal information and sensitive information.

9.2. How we retain and dispose of your personal information

We store and retain the information we collect securely in accordance with the *Public Records Act 2023* and relevant retention and disposal schedules.

We retain personal information only for as long as it is required for the purposes for which it was collected or to comply with legal and regulatory requirements. Once your personal information is no longer required, or has been identified as not belonging to you, it will be securely disposed of, by methods including:

Methods of secure disposal may include:

- Secure deletion of electronic records
- Shredding or secure destruction of physical records, and/or
- De-identification of personal information, where appropriate.

9.3. Getting your information

Individuals have the right to access the personal information that the department holds about them either informally, under our [Administrative Release Policy](#) or formally, under the *Right to Information Act 2009* (RTI Act).

You may also request to amend your personal information. The department will take reasonable steps to correct any information that is inaccurate, incomplete, out-of-date or misleading.

The department may refuse your request to access or amend your personal information, but you will be provided with a reason for our decision and, in the case of an amendment, we will place a note with your personal information indicating that you have disputed its accuracy.

We aim to provide as much information as quickly as possible. To apply to us for access to your information, you can apply online at www.rti.qld.gov.au, or you can contact our Right to Information and Privacy Team on (07) 3738 9893 or by email to RTIAdministration@justice.qld.gov.au

Where you are applying under the RTI Act for access to your information held by us, you will need to provide RTI and Privacy with evidence of your identity. To find out more, go to our [Right to Information and Privacy webpage](#).

9.4. Making a complaint

Through education and regular messaging, we make our expectations about how your personal information should be managed clear to our officers.

Sometimes, despite our best efforts, we make mistakes which lead to unauthorised use or disclosure of your information.

Our officers must comply with our Mandatory Data Breach Notification Policy and Procedure and are aware they must report all data breaches as soon as possible.

This sometimes means our RTI and Privacy team are often aware of a breach before you are.

We will notify you if we identify a data breach involving your information which will likely cause serious harm. If we don't have your contact information, we will publish an online statement or take other reasonable steps to make the data breach as widely known as possible.

We do this to help you take any additional actions you can to protect your information, such as changing a password or contact information and to comply with our obligations under section 73 of the IP Act.

We are committed to protecting and respecting your privacy. If you become aware of any act or practice which interferes with your right to privacy, you can make a complaint to us through our RTI and Privacy team by emailing us at privacy@justice.qld.gov.au, or calling (07) 3738 9893.

You can also make a privacy complaint to us by lodging your complaint on our [Compliments and Complaints](#) page. We manage our privacy complaints in accordance with our Information Privacy – [Complaints and Breaches Investigation Procedure](#). If you would like assistance with making your complaint, or if you've got any questions about how we manage your personal and sensitive information, you can reach our RTI and Privacy team by email to privacy@justice.qld.gov.au, or by phone to (07) 3738 9893.

We will only use and disclose your complaint information as allowed under the IP Act or under another Australian law or court order.

9.5. Correcting your information

Blue Card Services:

- If you wish to correct or amend your personal information, please visit the [Contact Us](#) page on our Blue Card Services website or by or calling Blue Card Services on 1800 113 611.

Disability Worker Screening:

- If you wish to correct or amend your personal information, you can do this online at contactus@workerscreening.qld.gov.au or the by calling the Disability Worker Screening hotline on 1800 183 690.