CHRISTEL NETWORKS & SOLUTIONS

PRIVACY STATEMENT

June 10th 2026

ChrisTel Networks & Solutions Pty Ltd – Privacy Policy

OVERVIEW

Privacy is important, and we take that responsibility seriously. We work hard to protect your personal information and uphold the security of your data at all times. This Privacy Statement describes how your personal information is collected, stored, used, and disclosed.

ChrisTel Networks & Solutions believes in collecting only the minimum information needed to verify your identity and provide your service. Unlike larger telcos that may collect driver licenses, passports, or other sensitive documents, ChrisTel uses trusted third-party identity providers, such as ConnectID (*ConnectID is a secure, privacy-preserving identity verification service developed under Australia's Digital ID framework*.) to verify your identity securely without storing full ID documents. We only receive a verified name and date of birth — nothing more. This privacy-by-design approach ensures your personal information stays protected and minimised at all times.

1. Purpose of this Privacy Policy

ChrisTel Networks & Solutions Pty Ltd ("**ChrisTel**", "**we**", "**us**", "**our**") is firmly committed to safeguarding the privacy, confidentiality, and security of personal information entrusted to us. This Privacy Policy outlines the manner in which we collect, handle, store, use,

disclose, and protect personal information in accordance with our obligations under the Privacy Act 1988 (Cth- Commonwealth) ("Privacy Act"), including the Australian Privacy Principles (APPs) set out in Schedule 1 of the Act.

By voluntarily opting in to the Privacy Act under section 6EA, ChrisTel Networks & Solutions acknowledges and accepts the full application of the Act and the APPs to all personal information we handle, irrespective of our annual turnover. We also comply with the Notifiable Data Breaches (NDB) scheme under Part IIIC of the Privacy Act, which requires us to assess, respond to, and notify eligible data breaches involving personal information that is likely to result in serious harm.

This Policy also reflects our obligations under:

- The Telecommunications Act 1997
- The Telecommunications (Interception and Access) Act 1979
- The Telecommunications Consumer Protections (TCP) Code C628:2019
- The ACMA regulatory framework
- The TIO complaints handling requirements
- The ConnectID Trust Framework and associated privacy and security standards

ChrisTel Networks & Solutions Pty Ltd adheres to the principle of data minimisation as required under the Australian Privacy Principles (APP 3 – Collection of Solicited Personal Information). We do not collect personal information beyond what is reasonably necessary for:

- Providing telecommunications services
- Supporting and maintaining customer accounts
- Meeting regulatory obligations
- Verifying identity for service activation
- Responding to customer enquiries

ChrisTel Networks & Solutions does not collect or store copies of identity documents such as driver licenses, passports, Medicare cards, or any other government-issued credentials.

2. Role of ConnectID in the Identity Verification

ChrisTel Networks & Solutions uses ConnectID, an accredited digital identity exchange, to perform identity verification in accordance with the ConnectID Trust Framework, the Privacy Act 1988, and the Australian Privacy Principles.

When you verify your identity using ConnectID:

- Your identity information is collected directly by your chosen Identity Provider (IdP), not by ChrisTel.

  Banks are the Identity Providers (IdPs) in ConnectID.

  Examples of IdPs:

- Commonwealth Bank
- NAB
- ANZ
- Westpac
- Other accredited digital identity providers

  These IdPs hold the customer's verified identity already (KYC).

- ChrisTel does not receive, access, or store your identity documents or raw identity attributes.
- ChrisTel receives only the minimum necessary verification outcome, which may include:
  - Pass/fail verification result
  - Confirmation of specific attributes (e.g., name, date of birth)
  - Transaction reference
  - Timestamp and audit metadata

This process ensures that identity information is handled securely and that ChrisTel Networks & Solutions only receives the least amount of personal information required to confirm your identity and activate your service.

3. Fallback Verification

If ConnectID is unavailable, ChrisTel may use an alternative accredited verification provider (e.g., RapidID). In such cases manually:

- ChrisTel still does not store identity documents
- Only verification results and required audit logs are retained
- All verification data is retained for 90 days, unless required by law

4. Purpose Limitation

Any personal information received through identity verification is used solely for:

- Confirming your identity
- Preventing fraud
- Complying with telecommunications regulations
- Activating or managing your service
- Keep personal information only as long as reasonably necessary, and
- Destroy/de-identify it when no longer needed.

ChrisTel Networks & Solutions does not use identity verification data for marketing, profiling, or unrelated purposes.

By engaging with our services, visiting our website (https://christel.com.au), or interacting with our systems, you acknowledge that you have read and understood this Privacy Policy and consent to the handling of your personal information in accordance with it.

As a small business voluntarily opting in to the Privacy Act, we treat your personal information with the highest level of care and transparency.

5. What personal information we collect

We may collect the following types of personal information:

Identity information

- Full name
- Date of birth
- Identification verification results (e.g., ConnectID, Pass/Fail flags)
- Contact details

Service information

- SIM activation details
- NBN service details
- VoIP/PBX configuration
- Call records (metadata only)
- Network usage information

Billing information

- Payment details
- Invoices and transaction history

Support information

- Tickets, emails, call logs
- Troubleshooting notes

Website and system information

- IP address
- Device information
- Cookies and analytics

When you visit our website or use our online systems, we automatically collect certain technical information such as your IP address, device details, browser type, and usage data.

We also use cookies and analytics tools to help us improve our website, maintain security, and understand how our services are used.

Note: ChrisTel Networks & Solutions does not collect sensitive information (such as health or biometric data) unless it is strictly necessary and you have provided your consent. At present, we do not require sensitive information to provide our services.

6. How we collect personal information

We collect information when you:

- Sign up for a service via ChrisTel Networks & Solutions website
- Verify your identity
- Contact support
- Use our website or portals
- Make a payment
- Interact with ConnectID or other identity providers

7. Why we collect personal information

We collect personal information to:

- Provide and manage your telco services
- Verify your identity
- Activate SIMs and NBN services
- Process payments
- Respond to support requests
- Meet legal and regulatory obligations
- Prevent fraud and security risks
- Improve our services

We do **not** sell personal information.

8. Identity verification (ConnectID)

ChrisTel Networks & Solutions uses ConnectID to verify customer identity.

We do not store:

- ID documents
- Photos of ID
- Scans or uploads

We only store:

- Verification result (pass/fail)

- Verification reference number
- Timestamp
- Required audit logs

Verification data is retained for **90 days**, then securely deleted unless required by law.

9. Disclosure of personal information

Disclosure of personal information We may disclose your personal information to:

- Telstra Wholesale (for service provisioning and network activation) through aggregators
- NBN Co **(**for NBN service qualification, activation, and fault management)
- Identity verification providers (such as ConnectID)
- Payment processors (for billing and transaction processing)
- Law enforcement agencies (when required or authorised by law)
- Regulators including ACMA**,** OAIC**,** and TIO
- Our technical partners, contractors, and service providers who support our systems, networks, and customer operations

We are required by law to provide certain customer information to the Integrated Public Number Database (IPND). This information is used for purposes such as emergency services, directory assistance, and law-enforcement requirements

10. Data storage and security

We store data in secure Australian data centres and trusted cloud environments with:

- Encryption in transit and at rest
- Access controls and MFA
- Audit logging
- Secure deletion processes
- Regular security reviews

We store personal information in secure Australian data centres and trusted cloud environments that meet industry-standard security and privacy requirements. To protect your information, we use a combination of technical, administrative, and physical safeguards, including:

- Encryption in transit and at rest to protect data as it moves across networks and when stored.
- Strict access controls, including role-based permissions and multi-factor authentication (MFA), ensuring only authorised personnel can access customer information.
- Audit logging and monitoring to track access, detect unusual activity, and support security investigations.

- Secure deletion and de-identification processes to ensure information is permanently removed when no longer required. Regular security reviews and system updates to maintain compliance, strengthen defences, and address emerging threats.
- Vendor and partner security assessments to ensure third-party providers handling data meet equivalent security standards.
- Network and application security controls, such as firewalls, intrusion detection, and vulnerability management.

These measures help ensure your personal information is protected against unauthorized access, misuse, loss, or disclosure.

11. Notifiable Data Breaches (NDB)

ChrisTel Networks & Solutions takes data breaches seriously. If we become aware of a data breach that is likely to cause serious harm to any individual, we will act quickly and transparently in line with the Notifiable Data Breaches (NDB) scheme.

If a breach occurs, we will:

a. Investigate immediately We assess what happened, what information was involved, and who may be affected.
b. Contain and mitigate the breach We take urgent steps to secure systems, prevent further access, and reduce potential harm.
c. Notify affected individuals If serious harm is likely, we will contact impacted customers directly with clear information about the breach and recommended steps to protect themselves.
d. Notify the Office of the Australian Information Commissioner (OAIC) We will lodge an official notification with the OAIC as required under the NDB scheme.
e. Review and prevent future incidents After containment, we analyse the cause and implement improvements to strengthen our security posture.

Although participation in the NDB scheme is mandatory for APP entities, we also commit to going beyond minimum requirements by responding promptly, communicating clearly, and taking proactive steps to protect our customers.

12. Access and correction of your information

You have the right to request access to the personal information we hold about you, and to ask us to correct any information that is inaccurate, incomplete, or out of date.

You may request:

- Access to your personal information We can provide you with the details we hold, such as your verified name, date of birth, contact information, and service details.
- Correction of your information If any information is incorrect or has changed, you can ask us to update it.

To make a request, contact us at: privacy@christel.com.au

We will:

- acknowledge your request
- verify your identity (to protect your account)
- respond within a reasonable timeframe, usually within **30 days**
- provide access in the format that is most practical and secure
- explain our reasons if we cannot provide access or make a correction (as permitted under the Privacy Act)

There is **no fee** to request access or correction, although we may charge a small administrative fee if you require copies of records.

13. Complaints

If you believe your privacy has been breached or you have concerns about how we handle your personal information, you can make a complaint.

a. Contact Us First

Email: privacy@christel.com.au We encourage you to contact us directly so we can resolve the issue quickly.

When you contact us, we will:

- acknowledge your complaint
- investigate the matter
- provide a written response within a reasonable timeframe
- outline any steps we will take to fix the issue

b. If You Are Not Satisfied with Our Response

Office of the Australian Information Commissioner (OAIC)

If you feel your concern has not been resolved, you may first escalate your complaint to the Office of the Australian Information Commissioner (OAIC) as OAIC's approach to early resolution using recognised External Dispute Resolution schemes.

For privacy-related complaints under the Privacy Act 1988 (Cth**)**. Website: oaic.gov.au The OAIC can investigate concerns about how organisations handle personal information.

Telecommunications Industry Ombudsman (TIO)

If your complaint relates to your telecommunications service and you believe it has not been resolved fairly. Website: tio.com.au The TIO is free, independent, and can require us to work with you to resolve the issue.

14. How can you contact us

If you have any questions about this Privacy Statement or how ChrisTel Networks & Solutions manages your personal information, please contact us on **1300 175 525** or email privacy@christel.com.au. You can also download a copy of this Privacy Statement at **https://christel.com.au/privacy**.

ChrisTel Networks & Solutions Pty Ltd

(ABN: 90 695 290 049)

Address: PO BOX 529, Riverstone NSW 2765

Privacy Contact: privacy@christel.com.au

APPROVAL AND AUTHORITY TO PROCEED

Approved by ChrisTel Networks & Solutions. This Privacy Statement is authorized for operational use across all services and customer interactions

Last updated: 10th June 2026