

PRIVACY POLICY

JMS Tech Newcastle

ABN: 82 423 623 805

Address: 20/70 Hanbury Street, Mayfield, NSW, 2304

Phone: +61 416 665 227 – **Email:** mateo@jmstech.com.au

Effective date: 1 July 2025

Version: v1.0 (1 Jul 2025)

Complaints: we aim to resolve within a reasonable timeframe (≈30 days). If you are not satisfied, you may escalate to the Office of the Australian Information Commissioner (OAIC) (tel. 1300 363 992 / online form). (APP 1.4(e))

Small business: we comply with the Australian Privacy Principles (APPs); if we are legally exempt, we voluntarily adopt these standards.

0. Introduction and Scope

JMS Tech Newcastle (“JMS”, “we”, “us”) handles personal information in accordance with the *Privacy Act 1988 (Cth)* and the *Australian Privacy Principles (APPs)*. Where the Privacy Act would not otherwise apply to us (for example, due to the small business exemption), we voluntarily adopt the APPs; where appropriate, we may formalise an opt-in under s 6EA. This Policy is made available free of charge on our website and, on reasonable request, in alternative (accessible) formats.

0.1 Who this applies to

Current and prospective customers, website visitors, and contact persons of suppliers and subcontractors. It applies to “personal information” that identifies you or could reasonably identify you. It does not apply to aggregated or anonymous data, nor—so far as permitted by law—to employee records held by private-sector employers (see the applicable exemption).

0.2 Anonymity and pseudonymity

Where lawful and practicable, you may communicate with us without identifying yourself or by using a pseudonym (for example, for general enquiries). We may need your identity to perform on-site services, meet legal obligations, or issue tax documentation.

0.3 Relationship with other documents

This Policy sits alongside our Terms and Conditions, Warranty/Commercial Benefits Policy and service-specific notices. In the event of conflict, applicable law and the APPs prevail. (APP 1 — open and transparent management.)

0.4 Overseas disclosures

We will indicate in this Policy if it is likely that personal information will be disclosed to overseas recipients and, where practicable, the countries in which they are located (see “International transfers” and the “Suppliers Annex”).

0.5 Privacy contacts and complaints

Contact details for the Privacy Officer and the complaints process (including the option to escalate to the OAIC) appear in the header of this Policy (see “Complaints”). We will handle your complaint within a reasonable time under the *Privacy Act 1988 (Cth)*.

1. Information we collect

We collect only the personal information reasonably necessary to deliver our services and operate our business, by lawful and fair means, and preferably directly from the individual where practicable.

- a) **Contact/identification data:** first and last name, email, phone, postal and billing address; job title and company where you act as a contact for a corporate customer.
- b) **Technical and service data:** hardware and OS details, configurations, issue descriptions, timestamps and duration of diagnostic sessions, a record of whether a **Diagnosis** (reasonable identification of cause) and an **Action Plan** were formulated to resolve the issue, technical logs and traces generated during support (including screenshots or session recordings only where necessary for diagnosis and with prior notice), and temporary credentials you provide for access. These credentials are handled under the principle of least privilege, stored (if applicable) in a secure manager, and revoked/deleted at the end of the job, unless a legal retention obligation applies.
- c) **Billing and transaction data:** service history, amounts and payment method. We do not store full card numbers; payments are processed via secure payment providers.
- d) **Communications data:** emails, tickets and messaging; and, where applicable, call recordings only with consent (see “Call recording” in this Policy). We may also record communication preferences (e.g., subscription/unsubscribe for marketing).
- e) **Automatically collected website data:** IP address, browser type, pages visited and timestamps, as described in “Cookies and analytics”. This may include IP address, device identifiers, online identifiers (e.g., cookies/advertising IDs) and serial numbers; in certain contexts these may constitute “personal information” when reasonably identifiable.
- f) **Applicant (HR) data:** if you apply for a job or send a CV, we may process identity and employment/education history. Note: the “employee records” exemption does not apply to applicants; we handle these data under this Policy.

Unsolicited information. If we receive information we did not request (e.g., personal files on a device during a repair), we will assess whether we could have collected it under this Policy; if not, we will destroy or de-identify it safely as soon as reasonably practicable. If retained, it will be handled under the rest of this Policy.

Sensitive information. We will only request sensitive information where strictly necessary (e.g., biometrics or health information contained on a device), with express consent unless a legal exception applies, and we will apply enhanced security measures.

Collection notice. At the time of collection (or as soon as reasonably practicable) we will inform you of purposes, consequences of not providing information, usual disclosures, and whether overseas disclosure is likely (including countries, where practicable), as set out in “Cookies and analytics”, “International transfers” and the Suppliers Annex.

Sources. We obtain data directly from the customer; we may also receive data from authorised third parties (e.g., your employer where you are a technical contact) or generate data during service delivery (e.g., technical logs).

Retention and destruction. Retention periods and methods of storage, de-identification and destruction are set out in §6 — Data Protection and Retention of this Policy.

2. Legal bases and purposes of processing (APP 6–7)

General rule (APP 6). We will use and/or disclose your personal information only for the **primary purpose** for which it was collected, or for a **secondary purpose** where an exception applies (e.g., your consent, or where the use/disclosure is reasonably expected and related to the primary purpose; for sensitive information, the relationship must be direct).

2.1 Primary purposes

- **Provision of technical services:** scheduling visits, diagnosis/support (remote, on-site, workshop), performing work and delivering outcomes.
- **Administration of the “No diagnosis, no charge (30 min)” commercial benefit:** verifying eligibility, evidencing elapsed time and the presence or absence of a Diagnosis/Action Plan, applicable billing, and resolving related disputes.
- **Administrative and contractual management:** quotes, work orders, invoicing, collections and warranty/after-sales support.
- **Operational security:** identity verification where necessary to deliver the service or protect systems/data.

2.2 Permitted secondary purposes

Uses compatible with the primary purpose where reasonably expected by you, or with consent where required:

- Service and experience improvement (review of incidents, aggregated/de-identified metrics).
- Quality and audit (internal controls, review of proper application of the “No diagnosis, no charge (30 min)” benefit, access traceability).
- Fraud prevention or unlawful activity, and protection of our rights or those of third parties where permitted by law.
- Transactional communications (e.g., job status notices, material service changes).

2.3 Direct marketing (APP 7 and *Spam Act 2003*)

We may use your data for direct marketing (e.g., newsletters or offers) only where: (a)

permitted under APP 7; or (b) we have your consent (express or, where the law allows, implied). You may opt out at any time; we will not use sensitive information for marketing without consent.

Practical rule (APP 7): if we collected your data directly and you would reasonably expect marketing from us, we may use it for that purpose provided there is a simple opt-out; if no such expectation exists or we did not collect the data directly, prior consent is required; sensitive information is used for marketing only with consent.

Spam Act/ACMA compliance: all commercial messages will include sender identification and a functional, free unsubscribe; we will process any opt-out within 5 business days.

2.4 Consent (definition and form)

Where processing requires consent, it may be express or implied, and must be voluntary, informed, current and specific, from a person with capacity. You may withdraw consent at any time (without retroactive effect on processing already lawful).

2.5 Uses/disclosures required or authorised by law

We may use or disclose information without consent where required or authorised by law (e.g., authority requests, crime prevention or investigation, or to mitigate a serious threat to life, health or safety), in line with APP exceptions and applicable legislation.

2.6 Sensitive information

We process sensitive information (e.g., biometrics or health data that may be on a device) only with consent or in the limited circumstances permitted by law, applying enhanced security measures.

2.7 Automated decision-making

We do not make solely automated decisions that produce legal effects or similarly significant effects. Any profiling is limited to permitted operational or marketing purposes and is opt-out.

2.8 Consequences of not providing information

If you choose not to provide information necessary for the primary purposes (e.g., contact data, essential technical access), we may be unable to provide the service or resolve the issue. Details and consequences are set out in the collection notice (APP 5) at the time of collection.

3. Cookies, tracking technologies and web analytics

3.1 What they are and when they are “personal information”.

Our site may use cookies, pixels/SDKs and similar technologies to operate the site, measure usage and, with your consent, offer advertising. Where these identifiers can reasonably identify you (alone or in combination), we treat them as personal information and apply this Policy (including APP 7 rules where used for direct marketing). We periodically review implemented technologies for compliance.

3.2 Categories of cookies trackers.

- **Strictly necessary:** essential for basic functions (e.g., security and access to protected areas).
- **Performance/analytics:** help us understand site usage and improve functionality (e.g., aggregated metrics).
- **Functionality:** remember user choices (language, region).
- **Marketing/advertising:** only with your consent; used to personalise ads or measure campaigns. Where used to target ads to individuals, we apply APP 7 (simple, transparent opt-out).

3.3 Notice and user controls (APP 5 and APP 7).

On first visit we display a banner allowing you to accept, reject or configure non-essential categories. You can change your choice at any time via “Cookie settings”. For electronic marketing communications, each message includes sender identification and a functional unsubscribe; we process any opt-out within 5 business days (Spam Act/ACMA).

3.4 Third-party analytics (e.g., Google Analytics 4).

We may use Google Analytics 4 (GA4) for aggregated usage statistics. GA4 reports that it does not log or store individual IP addresses and provides controls to disable, by region, granular location/device data collection or Google Signals. Analytics may nonetheless involve overseas disclosure (see §4).

3.5 Third-party cookies trackers.

Some third parties (e.g., analytics providers or ad networks) place their own cookies/SDKs. We do not control their practices and recommend reviewing their privacy policies. Where these technologies involve direct marketing or overseas disclosure, we apply APP 7 and APP 8 respectively (including providing opt-out and taking reasonable steps before any transfer).

3.6 Settings and opt-out alternatives.

In addition to our site’s cookie panel, you can: (a) adjust your browser to block/delete cookies; (b) disable personalised ads and Google Signals in your Google account (if applicable); and (c) opt out of direct marketing at any time via unsubscribe mechanisms (Spam Act/ACMA).

3.7 Enhanced transparency (APP 5).

In our collection notice we indicate the purposes of each cookie category, whether provision is mandatory or optional, the consequences of not providing data and, where practicable, the destination countries of involved providers (also listed in the Suppliers Annex).

3.8 Targeted advertising and pixels.

If we use tracking pixels (e.g., from social platforms) to personalise ads, we comply with APP 7 (including a simple opt-out) and periodically review these components to ensure suitability and proportionality.

4. International transfers of data (APP 8)

General framework. Where we disclose personal information to an overseas recipient, we will take reasonable steps to ensure that recipient does not breach the APPs; additionally, if an overseas disclosure occurs, we may be accountable for the acts or practices of the recipient that, if done in Australia, would breach the APPs (except APP 1).

Use vs disclosure (cloud/hosting). Providing data to an overseas provider solely for storage or processing under our effective control may, in some cases, be considered “use” and not “disclosure” (e.g., a contract limiting purposes to storage/support, subcontractors bound by the same obligations, and effective control over access/deletion). We nonetheless apply APP-8-equivalent measures as good practice.

4.a Possible processing locations

We may host or process data via providers located outside Australia (e.g., cloud services, support/ticketing, analytics or communications). Likely countries are indicated in the **Suppliers and Countries Annex** and will be updated as applicable.

4.b Reasonable steps before disclosure

Before any overseas disclosure, we take **reasonable steps**, including (as applicable):

- Due diligence on the recipient/country’s legal framework and controls.
- Binding contracts requiring protection at least substantially similar to the APPs and audit/security rights (including sub-processor management).
- Technical/organisational controls (encryption, access control, data segregation, deletion).
- Accessible complaint mechanisms for individuals.

These measures align with OAIC standards under APP 8 and accountability under s 16C.

4.c Informed consent (APP 8.2(b) exception)

If, in a specific case, we require your consent to disclose to an overseas recipient without applying APP 8.1, we will inform you expressly and in advance of the consequences: that APP 8.1 will not apply, that we will not be responsible under the Privacy Act for the recipient’s acts, and that redress may not be available in that jurisdiction. We will proceed only if you consent, and you may later withdraw consent.

4.d Other legal exceptions

We may disclose without applying APP 8.1 where required or authorised by an Australian law or a permitted general situation (e.g., to mitigate a serious threat to life or health), under the Privacy Act. These exceptions are limited and applied restrictively.

4.e Recent legislative changes (APP 8.2(aa) and 8.3)

From 11 December 2024, a new regulatory exception applies: if regulations prescribe that a recipient is subject to a law or binding scheme with protection substantially similar to the APPs and accessible enforcement mechanisms, APP 8.1 “reasonable

steps” are not required. We will list in the Annex any prescribed country/scheme we use.

4.f Information rights and transparency

You may request: (i) the countries where your data are stored or processed; (ii) the security measures applied; and (iii) the basis enabling each overseas disclosure (APP 1/APP 5). Our collection notice will also state if overseas disclosure is likely and, where practicable, the countries involved.

5. Sharing personal information (APP 6, APP 7 and APP 8)

General rule (APP 6). We disclose personal information to third parties only where necessary and consistent with the primary purpose of collection, or where an exception applies (e.g., your consent, or a reasonably expected, related secondary purpose; for sensitive information, the relationship must be direct). In all cases, we limit information to the minimum necessary.

Contractual and security controls. We require our suppliers and subcontractors to: (i) keep information confidential and use it only for the commissioned purpose; (ii) implement appropriate security controls; (iii) manage sub-processors under the same obligations; and (iv) delete or return information at the end of the engagement. Where the recipient is overseas, we apply APP 8 “reasonable steps” (see §4).

5.1 Categories of recipients

- a) **Technical suppliers and subcontractors.** Technicians/specialists assisting us (e.g., data recovery, field installations, remote support).
- b) **Manufacturers/distributors.** To manage parts/equipment warranties, we share only what is strictly necessary (customer identification and contact, model/serial and fault description).
- c) **Infrastructure and software.** Cloud services, ticketing, **timekeeping/session logs**, billing, communications and analytics processing data on our behalf and under our instructions (see §4 regarding locations and measures for overseas recipients).
- d) **Professional advisers.** Our lawyers, auditors or accountants where required for advice or compliance, including verifying proper application of the “No diagnosis, no charge (30 min)” benefit.
- e) **Authorities and legal compliance.** Where required or authorised by law, or in permitted situations (e.g., to reduce or prevent a serious threat to life, health or safety), we may disclose to competent authorities. We assess legality/proportionality and document the request and our response.
- f) **Corporate transactions.** In a merger, acquisition or restructuring, we may share data with counterparties and advisers under confidentiality, limited to what the transaction requires.

5.2 Prohibitions and limits

- **No data sales or third-party marketing.** We do not sell personal data or disclose it to

third parties for their own marketing without your consent. If we conduct or facilitate any direct marketing, APP 7 applies (including simple opt-out).

- **Advertising and analytics.** Use of third-party cookies/SDKs for analytics or advertising is governed by §3; where it involves overseas disclosure, §4 (APP 8) applies.
- **De-identified data.** We may share aggregated or de-identified information (not reasonably identifiable) for statistics, service improvement or reporting; this is not “personal information” under the APPs.

5.3 Record-keeping and traceability

We keep an internal record of third-party disclosures containing, as reasonably practicable: date, recipient, purpose, legal basis (APP 6, legal exception or consent) and, if applicable, whether it was an overseas disclosure (APP 8). This supports transparency and compliance.

5.4 Rights regarding third-party marketing (APP 7.6)

You may ask us at any time not to use or disclose your personal information to facilitate direct marketing by other organisations. We will honour that request free of charge and within a reasonable time.

6. Data Protection and Retention

6.1 Security measures (APP 11)

JMS Tech Newcastle implements reasonable technical and organisational measures to protect personal information against misuse, interference, loss, and unauthorised access, modification or disclosure. Measures include, as applicable: access control (MFA and least privilege), environment segregation, in-transit encryption (TLS 1.2+), at-rest encryption (e.g., AES-256), access logging and monitoring, patch and vulnerability management, encrypted backups, periodic testing and staff training. We also destroy or de-identify information when it is no longer needed, unless a legal exception applies.

6.2 Incident notification and Notifiable Data Breaches (NDB)

If we detect or suspect a security breach, we contain the incident, commence an expedited assessment and, within **30 days**, determine whether it constitutes an **eligible data breach** likely to cause **serious harm**. If confirmed, we will notify affected individuals and the OAIC as soon as practicable, detailing the nature of the incident, data involved, steps taken and recommendations to mitigate risk.

6.3 Suppliers and third parties (security and contract)

Where a supplier processes data on our behalf, we require confidentiality, limited use, appropriate security controls and sub-processor management under the same obligations, as well as deletion or return of data at the end of the engagement. If the recipient is overseas, we apply APP 8 “reasonable steps” and accountability under s 16C (see §4).

6.4 Retention periods

We retain data only as long as necessary for the described purposes or as required by

law. In particular:

- **Tax/business records (ATO):** generally ≥ 5 years.
- **Company financial records (*Corporations Act* s 286):** ≥ 7 years.
- **Records linked to the “No diagnosis, no charge (30 min)” benefit** (e.g., diagnostic timestamps and whether a Diagnosis/Action Plan was formulated): unless a legal obligation or open dispute exists, **up to 24 months** from last interaction for internal audit and dispute resolution, then secure deletion or de-identification.
- **Litigation/investigations/fraud:** until resolution or expiry of the applicable limitation period.

6.5 Limitations and shared responsibilities

We take reasonable steps under APP 11, noting that some risks depend on customer security practices (e.g., unsecured devices or networks, lack of backups). Nothing above limits our obligations under the Privacy Act or your rights; where the law requires us to retain data, we will do so even if you request deletion.

7. Individual rights (APP 12–13) and additional options

7.1 How to exercise your rights (verification and channels)

To process access or correction requests, we will reasonably verify your identity and accept requests by email or post (see header). We will respond within a reasonable time (our practice is within **30 days**). If the request is complex, we will keep you informed. (APP 12).

7.2 Access to your information (APP 12)

You may request access to personal information we hold about you. Where reasonable and practicable, we will provide access in the form requested; if not reasonable, we will offer alternatives (e.g., a summary). We may refuse access in limited cases set by law (e.g., serious threat to life/health, unreasonable impact on others’ privacy, frivolous requests, or information relating to ongoing legal proceedings). If we refuse wholly or partly, we will provide written reasons, complaint avenues and, where reasonable, an alternative form of access. (APP 12).

We may charge a **reasonable fee** only for facilitating access (e.g., copy/postage costs), not for making the request. We will inform you of any fee before processing.

7.3 Correction (APP 13)

We will take reasonable steps to correct information that is inaccurate, incomplete, out-of-date, irrelevant or misleading. You may also ask us to notify third parties to whom we previously disclosed your data; we will do so where practicable and lawful. We do not charge for requesting or making corrections. If we refuse to correct, we will explain the reasons in writing, how to complain and, if you request, we will attach a statement that you consider the information to be incorrect (“statement of claim”). (APP 13).

7.4 Direct marketing and withdrawing consent

You may opt out of direct marketing at any time (each message includes an unsubscribe option). You may also ask us not to use or disclose your information to facilitate direct marketing by others; we will comply free of charge. (APP 7).

7.5 Additional options (voluntary commitments)

Although the Privacy Act does not recognise a general “right to erasure”, we will consider deletion or restriction requests where: (a) the data are no longer needed for the stated purposes; and (b) no legal retention obligation applies (see §6 — Data Protection and Retention). You may also withdraw consent for processing that requires it (e.g., marketing), without retroactive effect on processing already lawful. (APP 11.2 and the APPs’ overall structure).

7.6 Costs

- **Access:** no charge to request; we may charge reasonable costs to facilitate access (we will notify you beforehand).
 - **Correction:** no charge to request or make corrections. (APP 12–13).
-

8. Notice of changes to this Privacy Policy

8.1 Nature of changes

We may amend, update or supplement this Policy to reflect legal/regulatory changes, operational or technological improvements, or variations in the services we offer. We will not implement changes that materially reduce your rights without legal basis or, where required, without obtaining your consent.

8.2 Publication and transparency

We will publish the updated version at jmstech.com.au/privacy, clearly indicating the effective date and a summary of changes. The Policy is available free of charge and, on reasonable request, in alternative formats.

8.3 Notice of material changes

If a change is material or may significantly affect your rights (e.g., new processing purposes, new categories of recipients, or new international transfers not previously covered), we will provide direct email notice to the registered address and/or a prominent site notice.

8.4 Advance notice period

For material changes we will provide at least **15 calendar days’** advance notice before they take effect, unless the change is required by law or needed to address an immediate security or privacy risk.

8.5 Commencement and effects

Amendments operate prospectively from the stated date. If a change introduces a secondary purpose you would not reasonably expect in relation to the original primary purpose, we will seek your consent before applying that change to data already

collected; if you do not consent, we will continue to process your data under the prior version to the extent necessary and permitted by law.

8.6 Version history

We will maintain a version history with effective dates; you may request copies of prior versions via the contact details in the header.

9. Government identifiers (APP 9)

9.1 General principle.

We will not adopt, use or disclose government-related identifiers (e.g., Medicare number, driver licence, passport, Tax File Number—TFN, Centrelink numbers/references) except where required or authorised by law, or where an APP 9 exception applies. The aim is to avoid such identifiers becoming “universal” and linking information across sources.

9.2 Permitted use/disclosure exceptions (summary).

We may use or disclose a government identifier only where an APP 9 circumstance applies (as relevant):

- identity verification or compliance with an agency;
- prevention, detection or response to fraud, unlawful conduct or a serious threat to life/health/safety;
- where required or authorised by an Australian law;
- where prescribed by regulation.

In all cases we limit handling to the minimum necessary and document it.

9.3 Operating rules.

- We do not adopt a government identifier as our internal customer ID (e.g., we do not use your Medicare or TFN as an account number).
- We will request/record such data only where necessary (e.g., managing a warranty with a manufacturer that requires a licence or passport for identity verification) and will use it exclusively for that purpose.
- We apply enhanced controls: restricted access, masking (e.g., last digits), encryption and minimal retention; we will delete or de-identify any copy when no longer required or on expiry of the applicable legal retention (see §6).

9.4 Specific rule for TFN.

When handling Tax File Number (TFN) information, we will comply with the *Privacy (Tax File Number) Rule 2015* in addition to the APPs (including APP 9). We will not adopt the TFN as our identifier and will limit its use to circumstances permitted by tax and privacy law.

10. Call recording and remote support (NSW)

10.1 Telephone calls

- **All-party consent.** In New South Wales we do not record private telephone conversations unless we have the consent of **all parties** to the call (valid express or implied consent), under s 7 of the *Surveillance Devices Act 2007 (NSW)*. Where applicable, we will inform you at the start of the call and seek your acceptance before recording. If you do not consent, we will offer non-recorded alternatives (e.g., email or ticket).
- **Limited exceptions.** The law provides narrow circumstances (e.g., protection of a participant's lawful interests), which we do not use for routine support/customer service recordings.
- **Use and retention.** Recordings are used only for service, quality and compliance, protected with reasonable measures against misuse, unauthorised access or disclosure, and deleted or de-identified when no longer required, consistent with APP 11 and §6 — Data Protection and Retention.

10.2 Remote support sessions (screenshots, logs and video)

- **Prior authorisation.** To provide remote support we may request installation of remote-access tools (or use existing ones) and, in specific cases, capture screens or record the session with your prior consent. We limit capture/recording to what is strictly necessary for diagnosis/resolution and ask you to close sensitive content before starting.
- **Legal alignment.** The *Surveillance Devices Act 2007 (NSW)* prohibits recording/monitoring the input/output of information from a computer on another's premises without the consent of the owner/controller; accordingly, we operate only with your authorisation and under your instructions.
- **Security and minimisation.** Logs and captures are safeguarded with reasonable measures (access control, encryption, minimisation), shared only with authorised personnel, and deleted or de-identified when no longer required, in line with APP 11 and §6 — Data Protection and Retention.

Non-recorded alternatives: If you prefer not to be recorded, you may request to proceed without recording or use alternative channels (email/ticket). We can still provide the service unless recording is strictly necessary to reproduce the issue or meet a legal obligation.

11. Minors and capacity to consent

Our services are not specifically directed to minors. The *Privacy Act 1988 (Cth)* does not set a fixed age for consent; we therefore assess case-by-case whether a person has sufficient capacity to understand and consent to the handling of their personal information.

- Where a person lacks sufficient capacity, we will seek consent from a parent/guardian, unless the law provides otherwise.
- We limit collection of minors' personal information to what is strictly necessary to deliver the service (e.g., repair of a family device) and apply enhanced security

measures.

- If you are a parent/guardian and believe we have handled a minor's data without appropriate consent, contact us (see header) to revoke consent, limit use or request deletion, to the extent permitted by law and our retention obligations.
- Where case-by-case assessment is impracticable, we may presume capacity from **15 years of age**, unless we have reasonable doubts about the person's ability to understand and consent.

12. Collection notice (APP 5) in forms and touchpoints

We will provide this APP 5 notice before or at the time of collection, or, if not practicable, as soon as reasonably practicable afterwards. At each form or collection point (website, email, tickets, phone), the notice will be clear and prominent and include, as applicable:

- Identity and contact details of the controller (JMS Tech Newcastle) and a reference/link to this Policy.
- Specific purposes of processing and whether any is for direct marketing (with consent/opt-out options).
- Consequences of not providing necessary information (e.g., inability to deliver the service).
- Usual third-party disclosures (suppliers, manufacturers, advisers, authorities) and, if overseas disclosure is likely, the countries involved where practicable (or a reference to the Suppliers Annex if published).
- How to exercise access and correction (APP 12–13) and how to lodge complaints (including the option to escalate to the OAIC).
- For forms involving cookies/trackers or analytics, a link to "Cookies and analytics" and to cookie settings.
- If collection is required or authorised by law, the applicable legal basis.
- If we collect data from third parties, from whom (or the type of source) and/or the circumstances of that collection.

Where an operational notice at a collection point differs from this Policy (for example, a new and limited purpose), that notice will prevail for that specific processing, without prejudice to the other terms of this Policy.

13. Definitions (Glossary)

- **APP / Australian Privacy Principles:** the set of 13 principles in the *Privacy Act 1988 (Cth)* regulating how covered entities handle personal information. Technology-neutral and principles-based; breaches may amount to an interference with privacy subject to regulatory action.
- **OAIC / Office of the Australian Information Commissioner:** the independent national regulator for privacy and freedom of information (FOI). Investigates and manages complaints, oversees compliance, issues guidance and exercises investigation/enforcement powers under the Privacy Act.

- **Personal information:** information or an opinion about an identified individual, or an individual who is reasonably identifiable, in any form (e.g., contact data, online identifiers, etc.). Whether someone is “reasonably identifiable” depends on context.
- **Sensitive information:** a subset of personal information receiving enhanced protection (e.g., health and genetic data, sexual orientation/practices, political opinions, religious or philosophical beliefs, racial or ethnic origin, union membership, criminal record and certain biometric data). Typically requires consent to process.
- **APP entity:** an “agency” or “organisation” to which the APPs apply under the Privacy Act (e.g., most government agencies and covered private organisations; some small businesses may fall outside unless they opt in).
- **Government-related identifier:** an identifier assigned by an agency/authority (e.g., Medicare, TFN, driver licence, passport) subject to APP 9 restrictions on adoption, use or disclosure by organisations.
- **Cross-border disclosure (APP 8) and “reasonable steps”:** before disclosing personal information to an overseas recipient, an entity must take reasonable steps to ensure the recipient does not breach the APPs; the entity may also be accountable (s 16C) for the recipient’s acts that would breach the APPs if done in Australia.
- **NDB / Notifiable Data Breaches scheme:** the regime requiring notification to the OAIC and affected individuals where a data breach is likely to cause “serious harm”. Entities must assess incidents promptly and generally determine within 30 days whether the breach is notifiable.
- **Consent:** may be express or implied; must be voluntary, informed, current and specific, from a person with capacity. Often required to process sensitive information or for secondary uses/disclosures that are not reasonably expected.
- **De-identification:** processes to ensure data are not reasonably identifiable (e.g., aggregation or technical/organisational techniques), noting the OAIC requires reasonable steps to prevent re-identification.