

Privacy and AI Use Policy

Version 1.0 | Effective 15 August 2026 | Sterling Volk

CONTENTS

01	About this policy	11	Client engagements
02	Our commitments	12	Our website
03	What we collect	13	How we protect information
04	How we collect it	14	Data breaches
05	Why we collect it	15	How long we keep it
06	Marketing and outreach	16	Access and correction
07	Who we disclose to	17	Complaints
08	Overseas disclosure	18	Contact us
09	How we use AI	19	Changes to this policy
10	Automated decisions		

01 About this policy

Sterling Volk builds communication infrastructure for growing, multi-site organisations. In doing that work we handle information about our clients, their people and sometimes their customers. We also use artificial intelligence as one of the tools of the trade.

This policy explains both. It covers:

- what personal information we collect, why we collect it and what we do with it
- how we protect it, and how you can access, correct or complain about it
- how we use artificial intelligence, what we will and will not do with it, and how we handle the intellectual property and content provenance questions that come with it

We handle personal information in accordance with the *Privacy Act 1988* (Cth) and the Australian Privacy Principles.

This policy applies to everyone we deal with: clients, prospective clients, contacts, website visitors, suppliers, subcontractors, and anyone whose information reaches us through the course of an engagement.

Terms used. "Personal information" means information about an identified individual, or one who is reasonably identifiable. "Sensitive information" includes health information, and information about someone's race, religion, sexual orientation, criminal record or union membership. It attracts higher protection.

02 Our commitments

1. We collect only what we need to do the work.
2. We do not sell, rent or trade personal information. Ever.
3. We do not use client information to train artificial intelligence models, and we do not use tools that do.
4. Every deliverable we release is authored, reviewed and approved by a person, and we take full responsibility for it.
5. We tell you what we are doing rather than burying it. If you ask a direct question about how your information is handled, you will get a direct answer.

03 What personal information we collect

Clients and client personnel

Name, role, employer, business contact details, correspondence, meeting notes, engagement records, billing and payment details.

Prospective clients and contacts

Name, role, organisation, business contact details, publicly available professional information, and records of our conversations and correspondence.

Website visitors

Information submitted through enquiry forms or newsletter sign-ups, and the technical information described in section 12.

Suppliers and subcontractors

Contact details, ABN, insurance and licensing details, and banking details for payment.

Applicants

Where we advertise a role or receive an approach, we collect the information supplied in the application.

Information encountered during an engagement

Our work involves reviewing client documents, websites, templates, intranets and communication systems. Those materials sometimes contain personal information about the client's staff, customers, residents, participants, patients or students. We do not seek this information out, we do not use it for our own purposes, and we handle it only as needed to perform the engagement and only on the client's instruction. Section 11 sets out how.

Sensitive information

We do not collect sensitive information unless it is necessary for an engagement and you have consented, or it reaches us incidentally within client material. Where sensitive information is not needed for the work, we ask the client to remove or de-identify it before providing documents to us.

04 How we collect personal information

Wherever reasonable, we collect personal information directly from you: in meetings and calls, by email, through our website, through a proposal or engagement process, or through the documents a client provides.

We also collect from public sources such as company websites, professional networking platforms, industry publications, tender portals and public registers, when researching organisations we may be able to help.

We may collect information about you from someone else, for example when a colleague refers you or a client nominates you as a project contact. If we do, and you would not reasonably expect it, we will tell you.

Anonymity. You can deal with us anonymously or under a pseudonym for general enquiries. For an engagement, we need to know who we are contracting with.

05 Why we collect and use personal information

We use personal information to:

- respond to enquiries and provide proposals and quotes
- deliver, manage and support our services
- communicate with clients and their teams during an engagement
- invoice, take payment and keep financial records
- research organisations and start relevant business conversations
- send occasional updates and insights, with an unsubscribe option in every message
- improve our services, methods and materials
- manage suppliers and subcontractors
- meet our legal, tax, insurance and record-keeping obligations

If we ever want to use your information for something outside these purposes, we will seek your consent or tell you first.

06 Direct marketing and business outreach

We contact senior people in organisations we believe we can help. If you receive an approach from us:

- we will identify ourselves and where we found your details
- every commercial electronic message we send includes a functioning unsubscribe facility, in line with the *Spam Act 2003* (Cth)
- unsubscribe requests are actioned promptly and permanently, and no further marketing is sent
- we do not sell or share your details with any other party for their marketing

You can opt out at any time by replying to any message or emailing [\[email\]](#). Opting out of marketing does not stop necessary communications about a current engagement.

07 Who we disclose personal information to

We may disclose personal information to:

- **Subcontractors and specialists** engaged on a project, such as developers, writers, photographers and production partners, all of whom are bound to confidentiality and to this policy

- **Service providers** that support our business, including cloud storage, email, project management, accounting, payment and artificial intelligence services
- **Printers and production suppliers**, where a deliverable is produced physically
- **Professional advisers**, such as our accountant, lawyer or insurer, where needed
- **Anyone else you have authorised**, or where disclosure is required or permitted by law

We do not disclose personal information for any other party's marketing purposes.

08 Overseas disclosure

Some of our service providers store or process information outside Australia, most commonly in the United States and the European Union. This includes cloud storage, email, collaboration platforms and artificial intelligence services.

Before using an overseas provider for client material, we take reasonable steps to satisfy ourselves that the provider's contractual terms require it to handle information consistently with the Australian Privacy Principles, including restrictions on use, retention and disclosure.

Where a client requires that its information be stored only in Australia, tell us at the start of the engagement and we will configure the engagement accordingly or decline the work. We would rather turn down an engagement than quietly breach a data residency requirement.

09 How we use artificial intelligence

Artificial intelligence is one of the tools we use to reduce communication debt for our clients. This section explains exactly how.

9.1 Principles

1. **Human authorship.** Every deliverable we release is authored, directed, reviewed and approved by a person. AI does not produce client work unsupervised.
2. **Disclosure.** Clients are told where AI has been used in a material way. We never represent a deliverable as entirely human-made when it is not.
3. **Confidentiality first.** Client information is not entered into tools that train on it, and not entered into consumer-grade tools at all.
4. **No decorative AI.** AI is used to improve the work, not to lower the standard or inflate volume.
5. **Traceability.** We keep a record of material AI use for each engagement, so any deliverable can be accounted for years later.

9.2 Where we use AI

We routinely use AI for

- research, synthesis and summarisation of publicly available material
- analysis of client-supplied documents during a Communication Debt Assessment
- drafting, restructuring and editing text under human direction
- auditing large document sets for inconsistency, duplication and drift

- building and testing AI-assisted knowledge tools, workflows and automations, where that is the agreed deliverable
- code, configuration and technical scaffolding for websites and systems

We do not use AI to

- produce final client-facing text, imagery or design without human authorship, revision and sign-off
- generate imagery presented as real people, real premises, real staff or real clients
- generate testimonials, case study quotes, reviews, statistics or citations
- make or substantially influence decisions about individuals
- process personal or health information, unless expressly agreed in writing under section 9.3

We always disclose before use

- any AI-generated image, illustration, voice or video appearing in a public-facing deliverable
- any AI system to be deployed into a client's environment where it will interact with staff or customers
- any use of AI involving personal or sensitive information

9.3 Client information and AI tools

- We use paid, business-tier AI services whose terms exclude customer inputs and outputs from model training. Consumer and free-tier services are not used for client work.
- Client material is never used to train, fine-tune or build any model, product or tool of ours.
- Personal information and health information are excluded from AI tools by default. Where an engagement genuinely requires their use, we obtain the client's written instruction first and agree the handling controls.
- Chat histories and uploaded files are purged from AI tools at the end of each engagement.
- Where a client has its own AI policy, approved tool list or data classification scheme, we work inside it. We ask for it at kick-off.

9.4 Intellectual property and ownership of AI-assisted work

What we retain

We retain ownership of what we bring to an engagement: our communication debt framework, assessment methodology, tools, templates, prompt libraries, workflow designs and reusable code. Clients receive a perpetual, non-exclusive licence to use these within their own organisation as part of the delivered work.

What the client owns

Everything created specifically for a client under an engagement is assigned to the client on full payment.

The limit we are upfront about

Australian copyright law protects work with a human author. Material generated wholly by a machine, with no meaningful human authorship, may attract no copyright protection at all. This is a limitation of the law, not of our work, and no supplier can honestly promise otherwise.

We manage it in three ways:

1. Every deliverable carries substantial human authorship: direction, selection, structure, editing and judgment. AI output is raw material, not the deliverable.
2. We assign all right, title and interest we hold in the deliverables to the client. We do not warrant that copyright subsists in a machine-generated element.

3. Where maximum protectability matters, for example a logo, wordmark or tagline intended for trade mark registration, we produce it without generative AI and confirm that in writing. Ask for this at scoping.

Third-party rights

We do not knowingly deliver material that infringes another party's copyright, trade mark, moral rights or confidential information. Deliverables are checked before release, and stock, font, image and software licences are documented and passed through to the client.

Moral rights

We do not present AI-generated material as the work of a named individual.

Client-supplied material

Clients warrant that logos, images, copy, documents and data they give us are theirs to supply and cleared for the intended use. We cannot verify the provenance of client-supplied material and rely on the client for it.

9.5 Content provenance and watermarking

AI-generated media increasingly carries embedded provenance signals. Two matter in practice: **Content Credentials (C2PA)**, a signed metadata record of what created a file and what edited it, now an international standard; and **invisible watermarks** such as SynthID, embedded in the file itself and designed to survive editing and re-encoding.

Our position:

1. We do not strip, alter, forge or defeat provenance metadata or watermarks in anything we deliver.
2. Where a deliverable includes AI-generated media, we tell the client at handover and record it.
3. We preserve Content Credentials through our production pipeline where the client's platforms support them. Many content management systems, social platforms and image optimisers strip this metadata on upload. We flag where that happens rather than claim provenance is intact when it is not.
4. We do not represent AI-generated media as human-captured photography, or the reverse.
5. Provenance metadata is a signal, not proof. Its absence does not prove content is human-made, and its presence does not prove content is accurate.

Regulatory context. European Union transparency rules for AI-generated content commenced on 2 August 2026, requiring machine-readable marking of synthetic content and disclosure of AI interaction. Australia does not yet have an equivalent statutory labelling regime, but in July 2026 the Australian Government announced mandatory national AI standards, a new Office of AI, and confirmed that no exemption will allow AI companies to train on Australian copyright material without permission, with draft legislation expected in 2027. We build to the higher standard by default and advise clients where labelling obligations apply to them.

9.6 Accuracy and human accountability

- All factual claims, figures, citations and legislative references in a deliverable are verified by a person against a primary source before release.
- AI-generated statistics or references are never included on trust.
- We take editorial responsibility for everything we release. AI is never offered as an explanation for an error.
- Where a deliverable is a system that will generate content on an ongoing basis, we design a human review step into it and document who owns that step after handover.

9.7 Subcontractors

Specialists we engage are contractually bound to this policy, including its confidentiality, disclosure, provenance and ownership terms. Sterling Volk remains the client's single point of accountability.

10 Automated decision-making

Sterling Volk does not use computer programs or artificial intelligence to make, or to substantially assist in making, decisions that could reasonably be expected to significantly affect the rights or interests of any individual. We do not use automated systems to assess job applicants, determine eligibility, set individual pricing or make decisions about any person.

Where we build an AI-assisted tool for a client, we design human review into it and document the controls at handover. Once handed over, the client is the operator of that system and is responsible for its supervision and for its own transparency obligations, including new Australian Privacy Principle 1.7, which commences on 10 December 2026 and requires covered organisations to disclose significant automated decision-making in their privacy policies. We will advise clients where we believe that obligation applies to a system we have built.

If our own practices change, we will update this section before any such use begins.

11 Client information during engagements

Most of what we handle is commercially confidential business information rather than personal information. Both are protected.

- Client material is used only to perform the engagement.
- Access is limited to the people working on that engagement.
- Where client material contains personal information about the client's staff, customers, residents, participants or patients, we act on the client's instruction, do not use it for any other purpose, and do not disclose it except as needed to deliver the work.
- We ask clients to de-identify or remove personal and health information before providing documents, where it is not needed for the work.
- We work within any client policy, approved tool list, data classification scheme or data residency requirement notified to us in writing.
- Where a client is subject to sector obligations, for example under aged care, NDIS, health or education regulation, we work to the standard the client requires and record it in the engagement terms.
- At the end of an engagement, client material is returned, archived securely or destroyed in line with the engagement terms.

12 Our website

Analytics

We use website analytics to understand how our site is used, including pages visited, approximate location, referring site, browser and device type. This is generally aggregated and not used to identify individuals.

Cookies

Our site uses cookies, which are small files stored by your browser. Some are necessary for the site to work. Others support analytics. You can block or delete cookies through your browser settings, though parts of the site may not function normally if you do.

Forms

Information you submit through an enquiry or subscription form is used to respond to you and, where you have opted in, to send occasional updates.

Third-party links

Our site may link to other websites. We are not responsible for their privacy practices and encourage you to read their policies.

13 How we protect information

We take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification and disclosure, including:

- multi-factor authentication on business systems
- reputable cloud services with encryption in transit and at rest
- access limited to those who need it
- device encryption, screen locks and current security updates
- confidentiality obligations on all subcontractors
- prohibition on consumer-grade and unvetted AI tools for client work
- secure destruction of physical material

No system is completely secure. If you believe your information has been compromised, contact us immediately using the details in section 18.

14 Data breaches

We maintain a data breach response process. If a breach occurs that is likely to result in serious harm, we will contain and assess it, notify affected individuals and the Office of the Australian Information Commissioner where required under the Notifiable Data Breaches scheme, notify the affected client without delay, and take steps to prevent recurrence.

15 How long we keep information

We keep personal information only as long as needed for the purpose it was collected, or as long as the law requires. Financial and engagement records are generally kept for seven years to meet tax and limitation-period requirements. Marketing contact records are kept until you unsubscribe or ask us to delete them. Client project material is retained, archived or destroyed in line with the engagement terms. Information no longer needed is destroyed or de-identified.

16 Accessing and correcting your information

You can ask us for the personal information we hold about you, and ask us to correct it if it is wrong, out of date or incomplete.

Email [\[email\]](#) with your request. We will verify your identity and respond within 30 days. Access is free in most cases. If a request requires substantial work we may charge a reasonable cost and will tell you before proceeding.

We may refuse access in limited circumstances permitted by the Privacy Act, for example where it would unreasonably affect another person's privacy or breach a confidentiality obligation to a client. If we refuse, we will explain why in writing and how you can complain.

If we hold information about you that was provided by a client, we will usually need to refer your request to that client, because they control it. We will tell you if that is the case.

17 Complaints

If you think we have mishandled your personal information, tell us. Email [\[email\]](#) with the details. We will acknowledge within five business days, investigate, and respond in writing within 30 days.

If you are not satisfied with our response, you can contact the Office of the Australian Information Commissioner:

- Website: oaic.gov.au
- Phone: 1300 363 992
- Post: GPO Box 5218, Sydney NSW 2001

18 Contact us

Privacy contact	Michel scott, Founder and Principal
Email	Consultant michael@sterlingvolk.com

19 Changes to this policy

We review this policy at least every six months, and whenever Australian privacy or artificial intelligence law changes materially. The current version is always published at [\[website\]/privacy](#). The effective date appears at the top of this page. Material changes are notified to current clients directly.

**Growth creates communication debt.
Sterling Volk measures it.**