Digital Risk Checklist for Community Legal Centres

A practical governance companion for boards and executive teams

Marzipan | 2026 Edition
A Digital Governance Companion for Community Legal Centres

INTRODUCTION

Why Digital Infrastructure Matters

Community legal centres have spent decades building trust. That trust is carried into every interaction — at the front desk, on the phone, in court, and increasingly, online. For many people seeking help, a centre's website is the first point of contact. It may be the only point of contact if geography, disability, or circumstance makes in-person access difficult.

The community legal sector places genuine care on how it communicates — ensuring that language, storytelling, and advocacy respect the dignity of the people it serves and avoid causing harm. Digital infrastructure now carries the same responsibility. The way an organisation manages its website, its online forms, its hosting arrangements, and its search presence either upholds or undermines those same values in practice.

Digital infrastructure — the systems, websites, hosting arrangements, and content that sit behind an organisation's online presence — is not simply a communications concern. It is a governance concern. It touches confidentiality, accessibility, reputation, and an organisation's ability to be found by the people who need it most.

This checklist is designed to help boards and executive teams build a working awareness of their organisation's digital risk profile. It is not an audit, and it does not require technical expertise. It is a structured starting point for conversation — a way to surface questions worth asking and to identify areas that may benefit from closer attention.

Five reasons digital infrastructure is a governance issue

- **Access to justice.** If a website is inaccessible, slow, or invisible in search results, people who need legal help may not find it. Digital barriers are service barriers.
- **Trust.** A broken form, expired certificate, or outdated information quietly erodes confidence — even when the services themselves are strong.
- **Governance oversight.** Boards are accountable for organisational risk. Digital risk — including security, privacy, and data handling — sits within that scope.
- **Community reach.** Search engines and online platforms determine who finds a service and when. This is directly relevant to mission delivery.
- **Confidentiality.** Online forms, client stories, and intake systems carry sensitive information. How digital tools are configured has direct privacy implications.

This guide does not suggest that centres are falling short. Most are doing thoughtful work with constrained resources and without dedicated digital staff. The purpose here is to support informed oversight — to help boards ask the right questions and give executive teams a shared framework for thinking about digital risk.

GOVERNANCE CONTEXT

Where Digital Governance Sits in Your Risk Framework

Digital infrastructure is sometimes treated as a standalone operational concern — something managed by a staff member, a web developer, or an IT provider, largely outside the board's line of sight. In practice, it intersects with several risk categories that boards are already responsible for overseeing.

- **Operational risk.** Reliance on a single person to manage digital systems, or the absence of documented processes for software updates and access control, creates operational fragility.
- **Reputational risk.** A broken form, outdated information, or a slow and unreliable website can quietly erode trust — with clients, funders, and referral partners.
- **Confidentiality and privacy.** Online intake forms, client stories, and document handling all carry privacy obligations. How digital tools are configured has direct implications for compliance.
- **Service accessibility.** If the website cannot be used by people with disability, or is not visible in search results, the organisation's capacity to deliver services is reduced.
- **Organisational trust.** Digital presence contributes to the overall credibility of an organisation. Funders, peak bodies, and community partners form impressions based on what they find online.

Digital governance does not sit outside these areas — it runs through all of them. The risk areas in this checklist are structured to reflect those intersections, and to support boards in asking questions that are relevant to their broader governance responsibilities.

GETTING STARTED

How to Use This Checklist

This document is structured as a series of risk areas, each containing board-level questions, common risk signals, and a brief explanation of why the area matters. It is designed to be worked through at a governance level — either by a board committee, in an executive team meeting, or as preparation for a more detailed review.

For each risk area, consider where your organisation sits using the following three-point framework:

- **Green — Confident —** We understand this area and have appropriate arrangements in place.
- **Amber — Unsure / Needs review —** We are uncertain, or this area has not been reviewed recently.
- **Red — Requires attention —** We are aware of a gap or concern that needs to be addressed.

There is no expectation that every area will be green. In many under-resourced organisations, amber is the honest and reasonable starting position — and that is a useful thing to know. The value of this exercise lies in building a shared, accurate picture of where digital risks sit, so that decisions about resourcing and attention can be made thoughtfully.

A summary scorecard is provided at the end of this document to support governance reporting.

RISK AREA 01

Security & Hosting

A community legal centre's website and associated systems hold or facilitate access to sensitive information. Even where client data is not stored directly on the website, the website itself — if compromised — can be used to mislead, intercept, or harm the people who rely on it. Hosting arrangements, software maintenance, and access controls are foundational to digital security.

Board questions to consider

- Who hosts our website, and do we have a current contact for that provider?
- Is there a documented process for how website software and plugins are updated?
- Who holds administrator access to the website, and is that list current?
- When were our website backups last tested?
- Is there a clear understanding of who is responsible for website security — internally or through an external provider?
- Has any security review or audit been conducted on our website in the past two years?

Common risk signals

- The website is hosted on a shared platform with no clear security responsibility.
- Website plugins or themes have not been updated in more than three months.
- Former staff or volunteers retain active administrator logins.
- Backups exist but have not been tested or verified.
- There is no SSL certificate, or the certificate is expired (site shows as 'Not secure').
- The organisation relies on a single person to manage website security, with no documented succession or handover plan.

Why this matters

A compromised website can redirect clients to harmful content, expose incomplete intake data, damage organisational reputation, or result in regulatory consequences. Security gaps are often invisible until something goes wrong. Clear governance of hosting arrangements and access controls is a basic duty of care.

RISK AREA 02

Accessibility & Inclusive Design

Accessibility is not a technical nicety — it is an access to justice issue. If a centre's website cannot be used by someone with a visual impairment, someone using a screen reader, or someone accessing the internet on an older mobile device with a slow connection, then that centre has created a barrier to its own services. The people most likely to need legal help are also more likely to face digital barriers.

The Web Content Accessibility Guidelines (WCAG) provide an internationally recognised framework for accessible digital content. Australian government services are expected to meet WCAG 2.1 AA standards, and the same principle applies to funded community services.

Board questions to consider

- Has our website been assessed for WCAG 2.1 AA compliance?
- Do we know how our website performs on mobile devices across different connection speeds?
- Is our content written in plain English, at an appropriate reading level for a general audience?
- Do our images have meaningful alternative text for screen readers?
- Are our forms, contact pages, and intake tools usable without a mouse (i.e., keyboard navigable)?
- Have we considered how people with low digital literacy access our services online?

Common risk signals

- The website has not been tested with a screen reader or accessibility checker.
- Content is written in legal or professional language without plain English alternatives.
- Forms rely on colour alone to communicate required fields or errors.
- Images contain text that is not available in any other format.
- The website is difficult to navigate on a mobile device.
- No consideration has been given to users with low English literacy or those using assistive technology.

Why this matters

People experiencing family violence, financial hardship, housing insecurity, or discrimination are overrepresented among those who face digital barriers. An inaccessible website does not turn away people at the door — it simply never appears in front of them. Accessibility is a legal and ethical obligation, and a practical one.

RISK AREA 03

Client Confidentiality & Online Storytelling

Community legal centres hold a position of deep trust with the people they serve. That trust extends into digital spaces — including the forms people complete online, the stories organisations share on their websites, and the way documents are handled in digital workflows.

Digital communication introduces confidentiality risks that are not always visible. Metadata embedded in uploaded documents, non-encrypted contact forms, and the use of client stories without robust consent processes are areas where careful governance is essential.

Board questions to consider

- Are our online contact and intake forms encrypted and transmitted securely?
- Do we have a documented consent process for sharing client stories publicly, including on our website and social media?
- Are client stories sufficiently de-identified to prevent re-identification?
- Do we have a process for removing metadata from documents before they are published or shared online?
- Is our privacy policy current, accurate, and written in plain language?
- Do staff understand the difference between encrypted and unencrypted communication channels when corresponding with clients?

Common risk signals

- The website uses a basic contact form with no clear indication of how data is handled or stored.
- Client stories are used in public materials without a documented, formalised consent process.
- Documents are published on the website without metadata being stripped.
- The privacy policy has not been reviewed since the organisation's website was last redesigned.
- There is no clear policy governing which communication channels are appropriate for client-sensitive matters.

Why this matters

For many clients, the decision to seek legal help is already difficult. A breach of confidentiality — even an inadvertent one — can cause serious harm and destroy the trust that is central to the centre's work. Online confidentiality governance is not separate from legal professional obligations — it is an extension of them.

RISK AREA 04

Search Visibility & Discoverability

When someone searches online for legal help, the results they see are shaped by search engine algorithms. A community legal centre that does not appear prominently in relevant search results is effectively invisible to the people searching for its services. This is not a marketing problem — it is an access to justice problem.

Search visibility is influenced by factors including the quality and clarity of website content, the technical health of the website, and whether the organisation's information is accurate and consistent across the web. Boards do not need to manage this directly, but they benefit from understanding that it requires active maintenance.

Board questions to consider

- Are our service pages written clearly enough for someone unfamiliar with legal processes to understand what we offer?
- Is our Google Business Profile (or equivalent) claimed, accurate, and regularly updated?
- Do we have a process for identifying and fixing broken links on our website?
- Is there a regular review of key service pages to ensure content remains current and accurate?
- Does our website load quickly on mobile devices?
- Are there any pages that are no longer relevant but still appear in search engine results?

Common risk signals

- Service descriptions are written in legal terminology rather than plain English.
- The Google Business Profile has not been updated since the centre's address, hours, or services changed.
- Broken links exist on the website and have not been identified or remedied.
- The website loads slowly, particularly on mobile devices.
- Outdated pages — including references to discontinued services or past staff — remain visible in search results.
- No one in the organisation has responsibility for monitoring how the centre appears in search results.

Why this matters

A person in crisis typically does not have the time or capacity to navigate a confusing website or to call multiple services. If a centre's web presence does not clearly communicate what it does and who it serves, it will be passed over — not by choice, but by circumstance. Search visibility is visibility to the people who need help most.

RISK AREA 05

Google Ad Grant Risk

Many community legal centres hold a Google Ad Grant — a programme that provides eligible not-for-profit organisations with up to USD $10,000 per month in Google Search advertising credit. When well managed, the Grant can meaningfully increase the number of people who find a centre's services through search.

However, the Grant carries ongoing compliance obligations. Accounts that fall outside Google's terms — through low click-through rates, non-compliant keywords, or inactivity — can be suspended. A suspended account provides no benefit, but a board may not be aware that this has occurred. Grant management warrants governance attention.

Board questions to consider

- Do we hold a Google Ad Grant, and if so, who is responsible for its management?
- Is the Grant account active and in good standing?
- Has the account been suspended at any point, and if so, was the cause identified and resolved?
- Are there governance reporting mechanisms in place to ensure the board is aware if the account becomes non-compliant?
- Is the Grant being used strategically, or is a significant portion of the available credit going unused each month?
- Are the keywords used in Grant campaigns aligned with the services the centre actually provides?

Common risk signals

- The Grant account was set up by a previous staff member and has not been actively reviewed since.
- The organisation does not know the current status of its Grant account.
- Less than 20% of the monthly credit is being utilised.
- Campaigns are running on broad or non-compliant keywords (e.g., single-word terms, or keywords unrelated to legal services).
- There is no staff or contractor accountable for Grant compliance and reporting.

Why this matters

The Google Ad Grant represents a meaningful resourcing opportunity for community legal centres. An inactive or suspended account is a missed opportunity to reach people at the moment they are seeking help. Board awareness of Grant status is a reasonable governance expectation.

RISK AREA 06

Reputation & Website Reliability

Reputational risk in a digital context is often slow and quiet. Unlike a public incident, the erosion caused by a broken contact form, a website that times out, or an SSL certificate that has lapsed tends to accumulate without anyone noticing — until a client, funder, or referral partner raises it, or until traffic data reveals a sustained decline.

For community legal centres, the stakes are particularly high. A person seeking help who encounters a website that appears unreliable may not try again. Technical drift — the gradual deterioration of digital systems without active maintenance — is a predictable risk that boards can help mitigate through appropriate oversight.

Board questions to consider

- Has our website been tested recently to confirm that all contact forms and intake tools are functioning correctly?
- Is our SSL certificate current and auto-renewing?
- Does the website present consistently across common mobile devices and browsers?
- Is there a process for identifying and removing outdated content — including references to past staff, closed programmes, or superseded information?
- Are website performance metrics reviewed on a regular basis?
- Who is responsible for monitoring the website's technical health, and how often is this reviewed?

Common risk signals

- No one has tested the contact form in the past six months.
- The SSL certificate has expired or is approaching expiry with no renewal plan.
- The website includes the names or biographies of staff who have since left.
- Information about services, eligibility, or locations has not been reviewed in the past twelve months.
- Website performance data (traffic, bounce rates, page errors) is not reviewed by anyone with oversight responsibility.
- The website loads slowly or inconsistently on mobile devices.

Why this matters

A website that does not work reliably communicates unreliability — regardless of how strong the organisation's services are. For people considering whether to seek legal help, first impressions matter. Technical reliability is a form of organisational integrity.

RISK AREA 07

AI Search & Emerging Visibility Risk

The way people find information online is changing. Search engines and AI-powered tools are increasingly generating direct answers to questions — drawing on website content and presenting it in summarised form. When someone asks ‘where can I get free legal help in Western Sydney?’, the answer they receive may come from a website the person never visits directly.

For a centre's services to appear accurately in these answers, the website needs to present information clearly and consistently: what the service does, who it is for, where it is located, and how to make contact. Centres whose web content is out of date or poorly organised may find that AI tools surface incomplete or incorrect information about them.

Board questions to consider

- Is it clear from our website — without navigating multiple pages — what services we offer, who is eligible, and how to make contact?
- Is our service information structured clearly enough for search engines and AI tools to understand what we do and who we serve?
- Is our content written and maintained by our organisation, kept current, and specific enough to reflect our actual services?
- Are there instances where AI search tools are surfacing incorrect or outdated information about our services?
- Does each key service page answer the most likely questions someone in need would ask — clearly and in plain English?

Common risk signals

- Service descriptions are vague or written in broad terms that do not reflect the specific help the centre provides.
- The website has not been reviewed for content accuracy in the past year.
- Service pages do not clearly state eligibility criteria, location, or how to access help.
- No one in the organisation monitors how the centre appears in online search results or AI-generated answers.
- Multiple pages cover similar topics without clear distinction, which can produce inconsistent results in search.

Why this matters

AI search is already shaping how people find services. Centres with clear, current, and well-organised web content are better placed to appear at the moments when someone is actively seeking help. This is not about technology for its own sake — it is about remaining visible and findable to the people the centre exists to serve.

SUMMARY

Governance Scorecard

Use the table below to record your organisation's position across each risk area. This scorecard is intended to support board reporting and to provide a starting point for planning. There is no pass or fail — the purpose is to build a shared, honest picture of where attention may be needed.

Risk Area	Status (G / A / R)	Date Reviewed	Notes / Next Steps
Security & Hosting			
Accessibility & Inclusive Design			
Client Confidentiality			
Search Visibility			
Google Ad Grant			
Website Reliability			
AI Search Visibility			

Interpreting your results

- **Mostly green:** Your organisation has strong digital governance foundations. Focus on maintaining current practices and scheduling regular reviews.
- **Mixed green and amber:** This is a common and honest position. Use the amber areas to prioritise where attention or resourcing is needed. Consider which areas carry the greatest risk to clients or the organisation.
- **Several amber or red areas:** This is useful information, not cause for alarm. Consider how digital risk areas can be incorporated into the organisation's broader risk framework, and whether an independent review would be helpful.
- **Mostly red:** The organisation would benefit from a structured review of its digital infrastructure. Prioritise security and confidentiality first, as these carry the most immediate risk.

We recommend revisiting this scorecard annually, or following significant changes to the organisation's digital systems, staffing, or services.

This checklist is intended to support internal reflection and governance discussions within community legal centres. It does not constitute professional advice and should be read alongside the organisation's existing risk frameworks and obligations.

Governance conversations about digital infrastructure are most productive when they are grounded in a clear, accurate picture of where things stand. For organisations that would benefit from a deeper independent review — one that goes beyond this checklist and produces a board-ready set of findings — the Marzipan Digital Capacity Diagnosis offers a structured starting point. It is designed to be practical, plainly presented, and proportionate to the context of community legal centre operations.

Further information is available at **marzipan.com.au**

Digital Risk Checklist for Community Legal Centres

2026 Edition | Marzipan | A Digital Governance Companion for Community Legal Centres