IT agreements

A guide to Information Technology (IT) agreements for community organisations

Oct 2025

justice connect

Contents

Part 1

Common types of IT agreements

Common types of IT agreements

This part of the guide covers common types of IT agreements:

- software licences and support agreements
- website agreements
- cloud services agreements
- internet service agreements
- telephone or other communication agreements
- hardware supply agreements
- website or software development agreements
- online marketing agreements

Disclaimer

This guide provides general information about common legal risks associated with IT agreements. This information is a guide only and is not legal advice. If you or your organisation has a specific legal issue, you should seek legal advice before deciding what to do.

Please refer to the full disclaimer that applies to this guide.

Terms used

In IT agreements, the organisation providing the IT products or services is often called the '**supplier**'. In this guide '**customer**' refers to the organisation which has entered into the IT agreement with the supplier.

Note – consumer contracts under the Australian Consumer Law

The Australian Consumer Law, set out in Schedule 2 to the *Competition and Consumer Act 2010* (Cth)) is the national law for consumer protections and fair trading.

Some IT agreements may also be consumer contracts or small business contracts under the Australian Consumer Law, in which case, your organisation may have rights under consumer guarantee and Unfair Contract Terms provisions in the Australian Consumer Law, in addition to its rights under the IT agreement itself.

More information – Consumer Guarantees and unfair contract terms

For more information, see our webpage on understanding contracts that covers Consumer Guarantees and unfair contract terms.

Software licences and support agreements

A software licence agreement is likely to be used when your organisation purchases or uses software, such as document production, case management or accounting software. ('Cloud services agreements' also often deal with software – these are discussed below).

Your organisation will usually not own the intellectual property rights in software and the supplier or a third party will own these rights. Your organisation therefore needs a licence (permission) from the supplier (or third party) to use the software. This will be set out in a licence agreement.

The agreement may include restrictions on:

- how you use the software (for example, no copying or modifying of the software), or
- the number of computers or users that can use the software

Licences for 'out of the box' software products are commonly expressed as 'non-exclusive' and 'non-transferable'. This means:

- the supplier can grant the same licence to multiple customers, and
- the customer can't transfer the licence to other persons (including other entities)

If your organisation requires the supplier to provide software support services for a period (such as assistance with using the software and any technical issues as well as help desk support), you can enter into a software support agreement. One agreement may cover both the grant of a licence to use the software and the provision of software support services and this is often considered to be the preferred model.

In some cases, your support agreement will include service levels guaranteeing, for example, minimum response times. This is important to ensure continuity, especially if the supplier's failure to provide the support services would significantly impact your organisation's activities.

Checklist of key considerations:	
• What is the duration of the licence? Does it automatically renew?	☐
• What is the scope of the licence granted? For example: – is the licence transferrable to other entities (such as within your organisation's corporate group)? – is the licence sufficiently broad to cover the ways in which you intend to use and benefit from the software?	☐
• What restrictions are imposed upon the use of the software (for example, modification)?	☐
• Are support services provided? If so, are they specified in sufficient detail such that the binding response and resolution times are objectively defined?	☐
• Does the agreement include the provision of updates and new releases for the software?	☐

- Does the software include artificial intelligence features? If so, are there clear terms around ownership and use of customer data? ☐
- If the software involves the supplier handling some of your organisation's data, are you comfortable with where your data will be stored and what the supplier can and can't do with your data? ☐

Note

It's important to understand the difference between an **update** and a **new release**.

Generally, an update is to fix errors or bugs in the software. New releases introduce new functionality to the software.

Note

Software licences are often presented as a 'clickwrap' agreement – that is, where users must click 'I accept' (or similar) before accessing the software.

These agreements are often offered on a 'take it or leave it' basis and tend to favour the supplier. It's important to review them carefully to understand your rights and obligations, particularly around payment, automatic renewal, and termination.

Website agreements

A domain registration agreement and a web hosting agreement are likely to be relevant if your organisation has a website.

Generally, to host a website, you will need:

- a domain name – the unique web address where visitors find your site which is rented from a domain registrar, subject to a **domain registration agreement**, and
- a web host – rented file space on a hosting company's web server where you put your website files (text, images and videos), subject to a **web hosting agreement**

If you have registered a domain name and hosted your website with the same supplier, you may be subject to just one set of terms, often labelled the supplier's **Terms of Service**.

These agreements may also supply other ancillary services to your organisation. These may include, for example, email services, and SSL certificates (SSL certificates increase security by encrypting data flowing between a website and its users).

Your organisation should make sure the agreement covers key elements such as the specification detailing the services and technologies required. This includes specifying the resources, such as storage capacity, bandwidth and processor power.

Checklist of key considerations:

- How is the agreement renewed for subsequent terms? When is the renewal date of the domain registration and the web hosting? ☐
- Who will procure the domain name – you or the supplier? ☐

- Is there a warranty for continuous access to the website? What are the consequences of website downtime? ☐
- Can the supplier vary the resources provisioned for the website under the agreement? Are there consequences to using excessive resources (for example, when you expect many site visitors at once during an event)? ☐
- Are there any limits on what kind of content you may publish (for example, sensitive or political information)? ☐

See the Office of the Australian Information Commissioner (**OAIC**) webpage on sending personal information overseas.

Cloud services agreements

A cloud services agreement is generally used where an organisation accesses or uses a supplier's hardware and software remotely (ie. the software is in the 'cloud').

Cloud computing involves the customer accessing a pool of computing resources such as software, networks, servers, storage, applications and services that are undertaken on the software. Therefore, a cloud services agreement is essentially an outsourcing arrangement where you outsource the provision of hardware and software.

The most common cloud services agreement is for 'Software as a Service' (**SaaS**) which provides ready to use software applications over the internet (for example, Microsoft 365, Canva and Salesforce). This model of software delivery is attractive to many not-for-profit organisations as you don't need to worry about the technology which supports the applications – you only pay for what you use, often on a subscription or per-user basis.

Note

Because a cloud services agreement encompasses the full technology solution, it's not usually accompanied by a support services agreement.

A key requirement for a cloud services arrangement will however be access to the internet via a telecommunications service.

The supplier may store, process or host your organisation's data, confidential or personal information under a cloud services agreement. If so, it's important to make sure data security is managed appropriately.

Suppliers of cloud computing often use other third party suppliers of cloud computing to provide supplementary resources or services, making the data you provide to a supplier harder to control. A cloud services agreement should appropriately deal with these 'subcontractors' or 'subprocessors'.

For business-critical software, it's important to ensure your organisation can continue operating in the event of a security incident disrupting the software. Cloud services agreements should include contractual commitments from the supplier to support continuity. These may include service levels (ie. obligations to perform against pre-agreed criteria), business continuity planning, data recovery, regular back-ups, data restoration, and disaster recovery arrangements.

Checklist of key considerations:	
• On what basis are you paying for the software (per user, monthly, per core)? Consider how you will track usage of the software to ensure you are not paying more than expected.	☐
• Where and how is your data stored, hosted or processed? Are there warranties to ensure data security?	☐
• Does the agreement involve data sent, accessed or otherwise handled outside of Australia? If your data comprises of personal or confidential information, it's recommended that the data stays in Australia. If personal information is to be sent, accessed or otherwise handled outside of Australia, you will need to consider your obligations under applicable privacy laws.	☐
• Is the supplier responsible for its subcontractors?	☐
• Are there express commitments to ensure continuity in services (for example, service levels, Business Continuity Plans (**BCP**), disaster recovery plans)?	☐
• If artificial intelligence features are used, are there controls to prevent the supplier from using your organisation's data for training or other purposes?	☐

Note

Cloud services agreements are often presented as a 'clickwrap' agreement – that is, where users must click 'I accept' (or similar) before accessing the software.

These agreements are typically offered on a 'take it or leave it' basis and tend to favour the supplier. It's important to review them carefully to understand your rights and obligations, particularly around payment, automatic renewal, and termination.

See the Australian Cyber Security Centre webpage 'cloud computing security considerations'.

Internet service agreements

An internet service agreement is used for an internet service provider (**ISP**) to provide internet access services to your organisation.

This agreement usually specifies the means by which internet access will be made available to your organisation, when access may be withheld and the extent of the ISP's liability for any access difficulties.

These agreements, like telecommunications agreements (below) are usually non-negotiable. As such, it's necessary to consider whether any risks in the agreement are acceptable to your organisation.

Telephone or other communication agreements

Telecommunication agreements are used where your organisation, for example, signs up for a landline service or buys a mobile phone.

Importantly, the unfair contract terms regime under the Australian Consumer Law is particularly relevant to these contracts, as these are often standard form consumer contracts. This means that (among other things) any terms which are considered to be unfair will be void and unenforceable.

The Telecommunications Industry Ombudsman (**TIO**) has a guidance note on telecommunications contracts.

For more information on unfair contract terms, see the Australian Competition and Consumer Commission's webpage on this subject.

Also see our fact sheet on unfair contract terms.

Hardware supply agreements

For lower-value hardware, hardware supply agreements are often made on standard supplier terms, with little room to negotiate. However, more complex or high-value hardware may involve bespoke contractual arrangements.

Hardware is typically either purchased or leased. A hardware purchase agreement is used where a customer purchases hardware or equipment (for example, computers or printers) and may cover delivery, installation and integration of the hardware or equipment, along with maintenance services. Alternatively, you may choose to use a hardware leasing agreement where you only have a short term need for such hardware.

While you may only be procuring hardware, you will likely require the accompanying software, firmware, and documentation necessary for its operation. Suppliers typically grant a licence to use such software, often subject to restrictions on reverse engineering, modification, and redistribution.

The most common cause of disputes in such agreements is where the hardware to be purchased is unclear, vague and open to interpretation. You must ensure that the hardware to be acquired is sufficiently detailed, including any performance specifications that the hardware must comply with.

The agreement may also deal with 'risk' and 'title', especially when dealing with delivery of the hardware. Risk refers to the risk of any loss or damage to the hardware, whereas title refers to legal ownership in the hardware.

Agreements prepared by the supplier often provide that title (ownership) passes to the customer only when the price is paid in full (this is often after the goods have been delivered), whereas the risk may pass once the hardware or equipment leaves the supplier's possession, or on delivery to the customer. This means that your organisation will bear the cost of loss or damage to the items during transit (when you have no control over the hardware), so it's recommended your organisation obtain appropriate insurances.

For more sophisticated hardware supply agreements or when procuring second-hand hardware, there may be a right for you to conduct acceptance testing – that is, to test the hardware after it has been installed and configured if it performs in accordance with the agreement.

As with other IT agreements with a maintenance or 'support services' component, it's important to make sure the services to be provided by the supplier are specified in sufficient detail and the scope is defined clearly.

Checklist of key considerations:	
• Do the specifications capture enough detail for the hardware to be procured?	☐
• When does ownership and risk pass to your organisation (keeping in mind that ownership and risk may pass separately)?	☐
• Is the supplier required to install the hardware? If so, what happens if installation takes longer or is more expensive than originally estimated?	☐
• Does your organisation have a right to inspect or test the hardware before accepting it? This may be particularly important when buying second-hand hardware.	☐
• Is maintenance of the hardware included? Where you opt out of maintenance, consider whether any warranties would be affected.	☐

Website or software development agreements

Under these agreements, the supplier agrees to develop a website or a piece of software.

In a website development agreement, a key issue for negotiation will be the specifications of the website and the agreement should make the extent to which the supplier is entitled to exercise creative discretion clear.

Your organisation should consider the appropriate payment structure to incentivise the supplier's performance. Developers often prefer to be paid monthly based on time spent, while customers usually prefer to pay only when key deliverables are completed. As a result, many software development agreements break the project into stages (such as planning, design, build, testing and implementation), with payments tied to successful completion of each stage. It may also be advisable to include testing requirements at each milestone which the software must pass before it is accepted. Ideally, no amounts should be payable to a supplier until the supplier has provided the services corresponding to such amounts (avoid upfront payment arrangements).

A key issue for negotiation will be ownership of intellectual property rights in the final product. Often, if the supplier retains ownership of the intellectual property rights, it will grant the customer a licence to use the developed product. You should ensure that such licence is sufficiently broad (for example, perpetual, irrevocable and includes a right to modify, enhance, sublicense).

To protect your organisation from any third parties claiming your website or software developed by the supplier infringes their intellectual property rights, you should ensure the agreement incorporates an indemnity for such claims (see the section below 'Indemnities').

These agreements can also involve the provision of support or maintenance services. Support services cover a range of activities, including bug fixes, the creation of new features or the introduction of new technology.

Checklist of key considerations:	
• Does the agreement clearly describe what the website or software is expected to do, including any design, functionality or performance requirements?	☐
• Are payment and the supplier's obligations tied to specific milestones or stages of development, with clear timelines and deliverables?	☐
• Is there a formal acceptance process or 'user testing period' outlined in the agreement which allows you to test the product and provides a timeline for the supplier to fix any defects?	☐

- Who will own the intellectual property in the final product? If the supplier retains ownership, does your organisation have a perpetual and irrevocable licence that allows it to use the software as required? Is there an indemnity to protect your organisation from third party intellectual property infringement claims? ☐
- Are support or maintenance services included? If so, are the scope, timeframes, and service levels clearly defined? ☐

For more information, see our guide to intellectual property law.

Online marketing agreements

Online marketing agreements are commonly entered into when your organisation engages third parties such as graphic designers, digital marketers, content creators, or social media agencies to promote your brand or cause across various online channels.

These agreements typically cover services such as brand development, advertising campaigns, email marketing, search engine optimisation (**SEO**), social media management, and production of creative materials (for example, videos, infographics, animations).

A key issue is ensuring the scope of services is clearly defined and tailored to your organisation's needs. Some agreements are structured around a fixed set of deliverables (for example, creation of a logo, three social media campaigns), while others involve ongoing retainers where the supplier provides services over a defined period (for example, monthly social media management).

It's important to ensure your organisation owns or has a licence to the intellectual property developed by the supplier. Unless otherwise agreed, the supplier will usually own the copyright in the materials they create, even if you have paid for them. Therefore, your organisation should ensure that it either owns the intellectual property in the deliverables or has a broad perpetual and irrevocable licence to use them. This is particularly important if your organisation wishes to reuse campaign materials across different fundraising drives or advocacy work.

These agreements should also address usage rights for third-party content incorporated into deliverables (such as stock images or background music), and who is responsible for obtaining appropriate permissions or licences. To address this, the supplier should indemnify your organisation in the event that any dispute over copyright arises (see section below 'Indemnities').

One of the biggest risks in launching a campaign is engaging in misleading and deceptive conduct, especially where the objective of the campaign is to persuade the public on a certain topic. Therefore, the agreement should contain controls to mitigate against this risk, including by instituting an approval process, requiring the supplier hold appropriate insurance cover, or requiring compliance with any relevant codes (for example, AANA advertising codes, AIMCO code of practice).

Any marketing agreements must require compliance with any applicable laws, which may include the *Privacy Act 1988* (Cth) (see section below 'Privacy'), the *Spam Act 2003* (Cth) and the Australian Consumer Law.

Checklist of key considerations:

- What is the scope of services to be provided? Are deliverables clearly described, including the number and type of materials to be developed? ☐
- Ensure deadlines are clearly defined. If the agreement is in the form of a retainer, ensure there is a mechanism to 'order' certain deliverables, and tie timeframes for completion to the date the 'order' was agreed. ☐

- Does the agreement oblige the supplier to comply with your organisation's brand guidelines? Does the agreement outline an approval process before content is published? ☐
- Who will own the intellectual property in the materials created? If the supplier retains ownership, does your organisation have a broad licence to use them? ☐
- Who is responsible for obtaining rights to any third-party content used (for example, stock images, fonts, music)? Is this supported by an indemnity from the supplier in the event of copyright infringement? ☐
- Is the supplier required to comply with applicable advertising and industry codes, such as the AANA codes and AIMCO Code of Practice (particularly for influencer campaigns)? ☐
- Does the agreement require compliance with all relevant laws? ☐

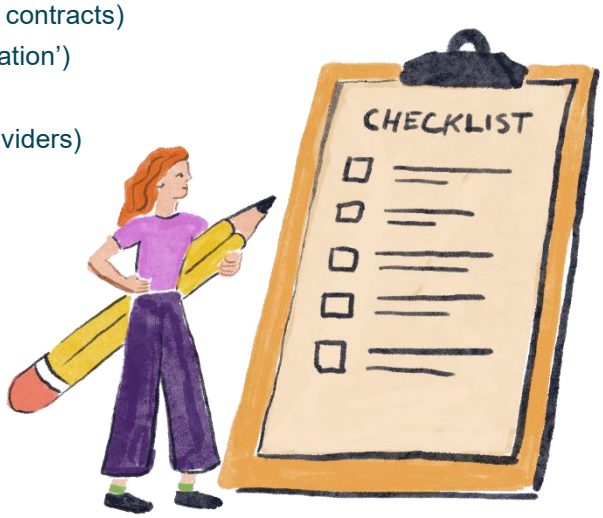
Part 2

Key legal issues with IT agreements

Key legal issues with IT agreements

This part of the guide covers key legal issues with IT agreements:

- when does the agreement start?
- payment
- automatic renewal of contract period (rolling contracts)
- description of products or services ('specification')
- incorporation of additional documents
- governing law and jurisdiction (overseas providers)
- changes to the agreement
- privacy
- confidentiality
- data security
- warranties
- service levels
- supplier's liability
- indemnities
- insurance
- artificial intelligence



Our list of key legal issues your organisation may need to be aware of when entering into an IT agreement is not a comprehensive list.

Depending on the agreement, there may be other legal matters to consider. However, the issues below are some of the most common or important.

An IT agreement is a type of contract so many of the legal issues relevant to contracts will apply here too. See our webpage on understanding contracts for general guidance on this.

When does the agreement start?

Make sure you know how and when the agreement actually starts and when your organisation is bound by it (ie. when you are legally required to fulfil any obligations under the agreement, in particular, payment of any fees).

Your organisation may become bound to an IT agreement by simply accessing or using the relevant product or service, or by clicking 'I agree' (or something similar) on a website. This means that your organisation may not need to formally sign the IT agreement before it becomes binding.

Note that the date the agreement starts is not necessarily the date that service delivery starts. Where relevant, you should check whether 'commencement date' and 'service start date' are clearly defined in the agreement.

What to do:

- Make sure the IT agreement uses the correct name for your organisation – this must be its full legal name and not any informal or abbreviated names, otherwise the agreement may not be valid
- Make sure the person making the purchase on behalf of your organisation:
  - is not specified as a party in their personal capacity, and
  - has the necessary authority to sign legal agreements on behalf of the organisation

What not to do:

- Don't start using IT products or services without first obtaining and reading a copy of the supplier's IT agreement
- Don't click 'I agree' before reviewing the IT agreement that applies

Payment

Payment clauses can differ significantly depending on whether the agreement relates to hardware (for example, the purchase of computers or servers) or software (for example, software licences or cloud services). The agreement should provide clear pricing terms and payment conditions that protect your organisation from unexpected cost increases or unreasonable invoicing practices.

Where hardware is being supplied, the agreement may include a single lump sum purchase price, potentially subject to variations due to factors such as foreign exchange movements, taxes, or changes in shipping costs. Suppliers may also seek to impose additional fees for services not expressly included in the agreement, such as urgent or remote support.

Software agreements often involve recurring licence fees, either as a one-off perpetual licence or as ongoing fees for fixed or renewable terms. Some agreements allow suppliers to unilaterally increase these fees mid-contract, which your organisation should try and avoid.

For agreements that cover IT projects (for example, developing your website or software), it's a good idea to ensure that payments are tied to the supplier's successful completion of project deliverables. This protects your organisation and incentivises proper performance by the supplier. You should try to avoid upfront payment plans in this context.

Larger suppliers may also provide not-for-profit discounted pricing. Ensure you ask the question to enjoy the benefits of any such pricing.

What to do:

- Check whether the supplier is entitled to vary pricing during the contract term. If so:
  - avoid clauses that allow the supplier to unilaterally change prices
  - if price variation is permitted, ensure it is limited to an agreed mechanism (for example, a fixed annual percentage or CPI-based cap), and
  - require that the supplier give advance written notice of any proposed increase, and ideally allow your organisation to terminate the agreement if the price increase is not acceptable
- Ensure the agreement clearly states when payment is due. For example:
  - prefer payment terms that start from receipt (not issue) of a valid tax invoice, and
  - if payment on delivery is required, consider negotiating to defer part of the payment until completion of installation or acceptance testing (if relevant)
- If payment is not a lump sum, consider whether you can negotiate a ceiling on the costs.
- For IT projects, try to ensure that payment is tied to the supplier's successful completion of project deliverables.
- Enquire if any not-for-profit fee discount applies and consider whether any not-for-profit specific terms apply (for example, whether there are requirements to verify your organisation's charity status periodically).

Automatic renewal of contract period (rolling contracts)

IT agreements often provide for automatic renewal of the initial contract period (for example, 12 months) and subsequent periods, unless the customer gives notice before that period expires that they don't wish to continue with the agreement. The customer is usually required to provide this notice within a specified timeframe or a 'notice period'.

If the notice is not provided within that specified period, the contract period will automatically renew for a further period and the customer will be committed to pay fees for that further period.

What to do:

- While automatic renewal provisions are designed to ensure service continuity (so that services aren't cut off when the contract period expires), your organisation should have a contract management system in place which alerts you in advance of when a notice of non-renewal is due.

  This is important as it allows for enough time to speak with the relevant stakeholders in your organisation to confirm if there is an ongoing need for the IT products or services.
- Ensure that each agreement's notice period is clearly recorded in your contract management system. Some IT agreements have unexpectedly long non-renewal notice periods.

Tip

A contract management system may be as simple as a spreadsheet you frequently update with a description of the contract (including a link to its terms), its price, the start and end date of any term (period), and any notice period which your organisation must comply with to terminate the contract before it automatically renews.

Description of products or services ('specification')

The agreement should detail exactly what is to be provided by the supplier (often called the 'specification').

An IT agreement prepared by the supplier may describe the products or services in insufficient detail, and at a high level only. It may not contain sufficiently detailed technical, operational or functional specifications which the product or service must meet.

An IT agreement may also state that the supplier only has an obligation to use 'reasonable endeavours' or 'best endeavours' to meet the product or service description. This type of wording means that their obligations are not firm.

Example

Your organisation enters into an agreement with a supplier to build its website at a cost of $5,000. It's important to your organisation that the website has a client portal with a private log-in for each individual client.

The agreement states that the supplier will use its best endeavours to build a private client portal with a unique log-in for each client. On viewing the final product it becomes clear that the client portal, although accessible only to clients, doesn't provide a private profile for each client as you had requested. The designer says that it became extremely complex to create private log-ins for each client and that despite using their 'best endeavours' under the agreement, it was not possible to achieve this within the timeframe of the agreement. Your organisation has to spend a further $2,000 to build this into its website.

What to do:

- Make sure the IT agreement sets out the supplier's performance obligations and the requirements and specifications for the products or services in sufficient detail. This should include:
  - what the supplier is supplying (ie. a description of the product or service being supplied and, in the case of products, the version number of the product)
  - how the product will be provided
  - what the performance requirements are
  - when the supplier is required to supply the product or service (including the start date of services and delivery date for products), and
  - where the supplier is to deliver the product or supply the services or where the services will be delivered from
- Look out for any clauses which say the supplier will use 'best endeavours' or 'commercially reasonable efforts' (or something similar) to perform certain obligations, and consider whether your organisation is willing to take this risk

Service levels

A service level agreement (**SLA**) is a key part of many IT contracts, especially for cloud services, support arrangements and managed services. It sets out specific performance standards that the supplier must meet, such as uptime guarantees, response and resolution times, and back-up or recovery commitments. SLAs are used to ensure the customer receives reliable, consistent service and that there are clear consequences where the supplier fails to perform.

Service levels should be drafted as binding commitments and not mere ‘targets’ or ‘reasonable endeavours’. Failure to meet SLAs should have enforceable consequences, including financial remedies (often termed ‘service credits’), rights to terminate the agreement, or both.

In most cases, the supplier will incorporate their own SLAs, if any. Service levels are application-specific and highly tailored to reflect the supplier’s commercial position on availability, response times and latency. Accordingly, it is unlikely your community organisation will be able to impose its own SLAs on the supplier.

What to do:

- Where possible, avoid vague language like ‘targets’, ‘reasonable efforts’, and ‘commercially reasonable endeavours’.
- Ensure service levels are properly monitored, preferably by requiring the supplier to report on its performance.
- Consider the consequences of failing to meet SLAs. Where there are no financial consequences (for example, service credits) or contractual consequences (for example, the right to terminate), SLAs may be ineffective.
- Beware of service credits as an exclusive remedy for performance failures. This can be high risk, especially if service credits are capped or don’t reflect the true impact of the failure.
- Some support services are only provided during certain hours (for example, during normal business hours). Check whether the hours stated are appropriate for your organisation’s operations

Incorporation of additional documents

An IT agreement may incorporate additional documents by stating that these other documents are also part of the agreement. These additional documents (such as **terms and conditions**, **privacy policies** or **dispute resolution procedures**) are often only available on the supplier's website or on request.

The effect of this is that:

- your organisation may be subject to additional obligations
- the supplier may have additional rights (which are not set out in the agreement itself), or

- the supplier may unilaterally vary the agreement without notice to your organisation (for example, by amending the terms referred to in a link to a website)

It may not always be clear whether an external document forms part of an agreement (for example, if it has simply been referred to without a clear intention that it is part of the agreement). In these cases legal advice may be necessary.

What to do:

- Look out for any clauses which aim to incorporate additional documents into the agreement. Where this occurs:
  - locate and read these additional documents before accepting the IT agreement
  - consider whether the agreement contains a variation clause which provides that no variation to the agreement is effective unless signed by both parties, and
  - download and keep a separate copy of any documents that are incorporated into the IT agreement (as website links may change over time)

Governing law and jurisdiction (overseas providers)

An IT agreement may specify that it's governed by the laws of a foreign country, for example, if the supplier is not based in Australia. This means the contract may be interpreted in a different way to how it would be interpreted under Australian law.

This means:

- your organisation's rights under the IT agreement could be interpreted differently from the position under Australian law
- any dispute arising under the IT agreement may need to be resolved under the laws of another country (often termed 'jurisdiction' for legal disputes), and
- your organisation may need to initiate or attend dispute resolution proceedings overseas. This can be protracted and costly

What to do:

- Before signing the IT agreement, look at the 'Governing Law', 'Jurisdiction' (or similar) clause, and consider whether it's acceptable to your organisation if a foreign governing law (or 'jurisdiction' for legal disputes) applies

Changes to the IT agreement

The IT agreement may allow the supplier to change the terms of the agreement, for example the description of the products or services, or the fees payable for the product or service. Changes to an agreement are often called 'variations'.

The IT agreement may allow the supplier to change the agreement at any time (or periodically) without your consent, or even without your knowledge (as such changes may sometimes only be published on the supplier's website).

This means there is no certainty for your organisation as to the supply of the products or services, or even as to the amount of fees to be paid.

What to do:

- Where possible, try to negotiate to limit the supplier's right to unilaterally vary the agreement. This is sometimes done by including a clause that requires any variation to the agreement to be made by both parties in writing.
- If negotiation is not possible, consider:

- whether there is a notice requirement in relation to changes to the agreement (that is, whether the supplier must give your organisation notice of the change), and
- whether your organisation is allowed to terminate the agreement if you don't accept the relevant change to the contract (and if so, whether your organisation will incur any liability or fees as a result of terminating). Note – if you are 'locked in' this may be considered an unfair contract term so it may not be valid

More information – Consumer Guarantees and unfair contract terms

For more information, see our webpage on understanding contracts that covers Consumer Guarantees and unfair contract terms.

Privacy

Privacy will be a very important consideration for many community organisations because they may be subject to privacy laws (or even be contractually bound to comply with privacy obligations) and hold personal or sensitive information about their service users, employees, volunteers or donors.

IT agreements can often include limited or no obligations on the supplier in relation to its handling of personal information (for example, names, contact details, credit card details) received from or accessed through your organisation.

Often the supplier only agrees to handle personal information in accordance with its own privacy policy, which is available in a separate document or website.

Caution – overseas providers

Cloud services and support services often involve:

- the supplier hosting and storing your organisation's data, which can include personal information
- personal information hosted in data centres outside of Australia, or accessed from overseas in the course of providing support services

Under Australian privacy law, if you outsource data services to an overseas provider you must take reasonable steps to ensure that the provider does not breach Australian privacy law as you will be accountable for those breaches.

Your organisation will also need to consider whether there is any constraint under agreements with third parties such as funding bodies, to transfer or disclose personal information to a supplier outside of Australia.

What to do:

- Be aware of your organisation's privacy policy and collection notices (notices you've provided individuals).
- Be aware of your organisation's privacy obligations.
- Consider whether the IT agreement allows your organisation to comply with its own obligations under applicable privacy laws and contracts.
- If there is a person in your organisation that deals with privacy matters (such as a 'privacy officer'), ensure they check the relevant sections of the agreement.

- Your organisation may want to conduct due diligence on the supplier. This can involve asking the supplier for details of its privacy law compliance, information governance, software security, access security and network security. You may need to ask the supplier to complete a security questionnaire.
- Consider whether the IT agreement contains appropriate protections, particularly if the supplier will host large volumes of personal, sensitive or confidential information, for example indemnities against any breaches of applicable privacy laws.
- If your organisation signs an agreement with an overseas supplier, the agreement should require the supplier to meet Australian privacy standards.
- Be aware and undertake due diligence on how your organisation and the supplier manages data breaches.

For more information, see:

- the Office of the Australian Information Commissioner (**OAIC**) webpage on sending personal information overseas.
- our webpage on privacy laws

Data security

The supplier may have access to your organisation's data during the time they provide the IT products or services. However, the IT agreement may state that the supplier is not liable for loss of data. It's therefore important to have appropriate data security measures in place.

Data security is linked to privacy but they are not the same thing.

While privacy is implemented through policies and procedures designed to safeguard personal information, data security is the technology and techniques used to prevent unauthorised access to and loss of data (for example access controls, regular backups and disaster recovery plans).

What to do:

- Carefully consider ownership and access rights to data. Consider having limits so that the supplier:
  - can only access and use your organisation's data for the purposes of providing the IT products or services to your organisation, and
  - can't use your organisation's data for any commercial or other purpose
- Consider the confidentiality of the data that is being provided to suppliers, specifically whether you have permission to provide the data to the supplier.
- Consider whether the agreement should include obligations and timeframes for the supplier to report security incidents or data breaches to you.
- If the supplier will host your organisation's data, identify whether the supplier is required under the IT agreement to maintain regular backups, which your organisation can request at any time and in the format required by your organisation.
- If the supplier is not required to maintain regular backups, your organisation should back up its own data.
- Consider whether the IT agreement allows your organisation to meet its record keeping and handling obligations.
- Consider when and how the data will be returned to your organisation upon completion or termination of the IT agreement.
- Consider whether the agreement should oblige the supplier to comply with certain information security frameworks, such as ISO/IEC 27001 (an international information security standard).

Note

When an IT agreement for cloud services expires or is terminated, your organisation may only have a short timeframe to retrieve your data stored by the supplier.

Retrieval after this timeframe may incur additional fees, or the supplier may delete the data permanently.

For more information, see our webpage on cyber security.

Confidentiality

It's important to consider any confidential information exchanged between your organisation and the supplier as part of the arrangement (for example, donor databases, business plans and financial information). Confidentiality overlaps with privacy and data security (see above sections) but is a distinct consideration.

Confidentiality clauses usually define what 'confidential information' is and how the parties to the agreement can use it. The clause will usually oblige your organisation or the supplier (or both parties) not to disclose confidential information to any third parties.

You should ensure that the definition of 'confidential information' is appropriate, given the type of confidential information that you expect to be protected under the agreement. Try to avoid vague language. It can be a good idea to explicitly list the categories of information that you want to cover.

If the confidentiality clause imposes obligations on your organisation over and above your usual processes for handling such information, you may wish to implement practical safeguards to ensure you don't make an accidental disclosure. This could be as simple as informing the people who will be handling the information of their obligations or maintaining a register of confidentiality agreements to ensure ongoing compliance and awareness.

Some types of information may attract additional regulation (for example, tax file numbers, credit history and electoral role information). This guide does not cover these types of information.

For more information, see our webpage on privacy laws.

What to do:

- If the agreement doesn't contain a confidentiality clause, consider whether you are providing the supplier with any information that you want to protect.
- Check the definition of 'confidential information' and make sure it's appropriate considering the information being shared between the parties.
- Consider whether there are or should be any permitted disclosures of the confidential information (for example, to your employees on a need-to-know basis).
- Is a time limit specified for the duration of the confidentiality obligation? Does it continue even after the agreement has ended? If not, do you want your confidential information to be protected for some time after the agreement is done?
- Does the agreement require the supplier to return or destroy your confidential information at the end of the agreement or at your request?

Note

In some circumstances, you or the supplier may have an obligation to keep certain information confidential due to the commercial or secret nature of the information itself or the circumstances in which the information was obtained. These obligations can arise even if there is no clause in the agreement which deals specifically with confidentiality.

For more information, see our guide to intellectual property law.

Warranties

A warranty is a guarantee to repair or replace a faulty product or service. It's important to understand the warranties your organisation is covered by if a defect is discovered in the products or services supplied.

An IT agreement prepared by a supplier often contains very limited warranties or repair or replacement obligations. Even if the supplier provides a warranty, there may be broad exclusions from this warranty.

Where the IT agreement concerns hardware or licensed software, the agreement will often specify a warranty period during which the relevant warranties apply, or during which the supplier agrees to repair or replace defective software or hardware at no additional cost.

For cloud software, warranties typically relate to the software's performance against agreed specifications. However, software is rarely free from defects, and it is common industry practice to accept that some bugs will exist. As a result, suppliers may only warrant that the software will be 'materially free from defects'.

Tip

Certain statutory guarantees are set out in the Australian Consumer Law which apply to supplies of some ICT products or services. If these statutory guarantees apply, they can't be excluded or modified by the IT agreement.

For more information about statutory guarantees, see the our webpage on understanding contracts.

What to do:

- If the IT agreement specifies a warranty period, consider whether it is sufficient, having regard to the timeframe during which defects are likely to be discovered.
- Consider whether a longer warranty period is needed, and if so, consider whether to buy additional support services from the supplier.
- Consider whether cloud software, at a minimum, should be 'materially free from defects'.
- Consider if you want warranties on updates and new releases, and whether the warranty period will start again after an update or new release is provided.
- Carefully read any exclusions from warranties and repair or replacement obligations.
- Make sure your organisation understands the circumstances where remedies will not apply (for example, a defect caused by your organisation's own modifications to the software or hardware).

Supplier's liability

Limitation of the supplier's liability

Under IT agreements, the supplier's liability is often limited to, or capped at, a specified amount. This means that if they don't fulfil their obligations under the agreement, they will only have to compensate the customer up to a certain amount, regardless of the actual loss caused. This amount is often set by

reference to the fees payable (so, for example, the supplier may have to forego a percentage of the fees payable under the agreement).

However, IT agreements often don't include a similar limitation or cap for the customer's liability, which means that your organisation's liability may be unlimited.

Example

A community organisation runs a small social enterprise which sells biodegradable picnic ware on an online platform. The social enterprise enters into a service agreement with a supplier to maintain its software and fix any technical errors. The supplier fails to fix a software error by an agreed deadline, which leads to the social enterprise missing out on a large order to the value of $3,000.

A limitation of liability clause in the service agreement states that – if the supplier fails to fix a software error, the supplier's liability is limited to $1,000. This means that the social enterprise will not be entitled to claim the full amount of its loss from the supplier.

Note that a limitation clause, depending on how far it seeks to limit liability, may be deemed unfair under the unfair contract terms provisions in the Australian Consumer Law.

What to do:

- Assess the overall risk of the transaction, the nature of the IT products or services provided and the potential liabilities your organisation may incur as a result of the supplier's failure to perform (including failure of the products or services).
- If the price payable under the IT agreement is low, this does not necessarily mean that the risk of loss or damage to your organisation would also be low.
- Look out for any cap or exclusion of liability by the supplier and consider if this is appropriate. Note – there may be different caps for different types of loss (for example, there may be a separate 'super' cap on loss arising from a breach of privacy, confidentiality or data security provisions).
- Consider whether any limitation of liability in the IT agreement impacts your organisation's insurance.

Note

If your organisation's liability is uncapped, you may wish to introduce, where possible, a clause which caps your organisation's liability. A common approach is to mirror the supplier's exclusion or limitation of liability clause. However, such clauses can be complex so you should consult a lawyer if you're unsure.

Exclusion of the supplier's liability

Under an IT agreement, the supplier may seek to exclude its liability for some types of loss suffered by the customer, meaning that it wouldn't have to pay any compensation in some circumstances.

Be aware that an agreement prepared by a supplier may seek to exclude liability for a wide range of events or losses. For example, an exclusion of liability clause may state that the supplier is not liable to compensate the customer for loss of profit, loss of revenue, loss of data or loss of reputation. The terms 'indirect' or 'consequential' losses are sometimes used to cover these types of loss, although the meaning of these terms can be unclear and this may lead to a disagreement over whether a certain type of loss should be compensated.

Example

Continuing the earlier example, the IT agreement between the social enterprise and its supplier also states that the supplier bears no liability for any loss of the customer's data.

The supplier does eventually fix the technical problem, but while it is doing this it accidentally deletes all the social enterprise's sales records for the previous six months. This data had not been backed up.

The social enterprise has to hire an IT consultant at a cost of $1,500 to retrieve the lost data. Under the wording of the agreement, the supplier wouldn't have to compensate the social enterprise for this.

What to do:

- Consider the particular types of losses your organisation may suffer and the types of claims your organisation may have, as a result of the supplier's default under the IT agreement. For example, would the result just be inconvenience or real financial loss?
- If the supplier is responsible for storing or hosting your organisation's data, and the supplier seeks to exclude its liability for loss of this data, assess the risk and take steps to mitigate such risk, paying special attention to any privacy obligations with respect to taking precautions to protect personal information. This could be, for example, by maintaining regular backups of your organisation's data and having robust data breach response plans.
- Where possible, try to negotiate 'carve outs' to the supplier's exclusion of liability. Customers often seek 'carve outs' for damage caused by the supplier's breach of its confidentiality, privacy, data security and intellectual property obligations under the agreement. Liability clauses can be complex so you should consult a lawyer if you're unsure.

Indemnities

An indemnity is essentially a promise to compensate the other party for loss or damage that they suffer as a result of a contract.

Most suppliers are willing to give only very limited indemnities. Such indemnities are often conditional on the customer notifying the supplier of any claim within a specified short period and allowing the supplier to control the defence or settlement of the claim.

Some IT agreements don't provide for an indemnity by the supplier at all.

Example

Your organisation signs an agreement with a supplier to design the organisation's website, including a new logo. A clause in the agreement says:

'*The supplier agrees not to design or develop any items that infringe patents, copyrights, trade marks or property rights of any person or entity. The supplier agrees to indemnify the customer against any such alleged or actual infringement and for any liability, debt or other obligation arising out of such infringement. This shall include legal fees and expenses. The supplier's total liability is limited to twice the fees due to the supplier under this agreement*.'

After your organisation's new website goes live it is contacted by another organisation which claims that your logo breaches its copyright and trade mark registration because it is confusingly similar to their own logo.

Your organisation has to engage lawyers to respond to the claim. Under the above clause, the supplier is responsible for these legal costs (as long as they don't exceed twice the fees the supplier is entitled to under the agreement).

What to do:

- Consider whether the terms of any indemnity are appropriate and consistent with your organisation's policies in relation to indemnities and the handling of claims
- Consider whether the supplier provides an indemnity against infringement of third party intellectual property rights. If it doesn't, your organisation may become liable for claims by third parties that the use of the IT products or services infringes that third party's intellectual property rights. If this is the case, you should consider whether this risk is acceptable to your organisation
- Consider whether your organisation has adequate insurance for any losses or risks not covered by the supplier.

In addition, the IT agreement may require your organisation to indemnify the supplier for various events or losses your organisation may cause. In many IT agreements, the risk of your organisation being liable under an indemnity may be low. However, if your organisation were to be liable under an indemnity, the financial consequences could be significant. Therefore, you should consider whether you're comfortable with the risk associated with any indemnities.

What to do:

- Conduct a risk assessment and consider the likelihood of your organisation's actions causing loss to the supplier. If your organisation gives an indemnity, this should be limited to issues or events your organisation can control. You should implement practical measures to mitigate the risk associated with any indemnities given.
- Consider whether an indemnity given by your organisation is limited to a specific amount. Where it is not, you should consider negotiating a 'cap' (a financial limit) to the indemnity. These matters can be complex so you should consult a lawyer if you're unsure.
- Confirm whether the provision of an indemnity in an IT agreement would impact your organisation's insurance cover.

Insurance

If your organisation grants access to its data to a service provider, you may want to consider including a cyber insurance clause which obligates the supplier to take out a cyber insurance policy which can compensate against losses resulting from cyber-attacks, ransomware, or data loss.

You may wish to consider taking on cyber insurance yourself. Other forms of insurance to consider include professional indemnity insurance, public liability insurance, and workers' compensation insurance.

For more information, see our guide to insurance and risk management for not-for-profit organisations.

Artificial intelligence

Artificial intelligence (**AI**) systems are increasingly embedded in IT products and services, and their use can introduce a range of legal risks. These risks span consumer protection, privacy, intellectual property, liability, and governance. **An IT agreement should clearly outline how AI systems are deployed, what data they use, and the responsibilities of both parties**.

Where AI systems are used to generate content, the agreement should address the risk of misleading or inaccurate outputs. This includes ensuring that any representations made by the AI system do not breach the Australian Consumer Law, particularly in relation to misleading or deceptive conduct. Organisations should also be aware of the risk of bias in AI outputs, especially where decisions may impact individuals based on personal characteristics.

AI systems often process personal or sensitive information. This raises privacy concerns under the *Privacy Act 1988* (Cth), particularly where data is used for profiling, automated decision-making, or training purposes. Agreements should include clear obligations on the supplier to comply with privacy laws and implement appropriate security measures. Organisations should also consider whether the supplier's data handling practices align with the organisation's own ethical standards and community expectations.

Intellectual property rights in AI-generated outputs are not always clear. The agreement should specify who owns the input and output data, and whether the organisation has rights to use, modify or commercialise the outputs.

Suppliers should also provide warranties and indemnities to protect against third-party infringement claims, particularly where AI is used to create public-facing content, such as educational materials or advocacy campaigns.

Liability for harm caused by AI systems (including financial loss, reputational damage or breach of contract) should be addressed in the agreement. This includes ensuring that the supplier's liability is not unreasonably limited and that appropriate indemnities are in place (for example, for inaccurate outputs, bias, or IP infringement).

What to do:

- Confirm whether the agreement clearly describes how the AI system will be used and what it is expected to do.
- Consider whether the agreement includes appropriate disclaimers or transparency measures to inform users when AI is being used.
- Assess whether the supplier warrants that the AI system complies with applicable laws, including privacy, data protection and consumer rights. If no such warranty is provided, consider whether this risk is acceptable to your organisation.
- Consider who owns the input and output data generated by the AI system. Ensure that usage rights are clearly defined and consistent with your organisation's data governance policies.
- Look out for any limitations on the supplier's liability for harm caused by the AI system. Consider whether these limitations are appropriate given the nature of the AI functionality and the potential risks to your organisation.
- Confirm whether the supplier is required to implement appropriate governance, oversight and security controls in relation to the AI system. This may include obligations around monitoring, auditing, and suspension of the system if necessary.
- Consider whether the supplier provides an indemnity for infringement of third party intellectual property rights in connection with the AI system.

For more information, see our guide Artificial intelligence and your organisation.

justice connect