Information Technology (IT) agreements

Legal information for community organisations

This fact sheet covers:

- common types of IT agreements
- key legal issues with IT agreements, and
- managing risks associated with IT agreements

Disclaimer

This fact sheet 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 fact sheet.

Terms used

In IT agreements, the organisation providing the IT products or services is often called the 'supplier'.

In this fact sheet ‘customer’ refers to the organisation which has entered into the IT agreement with the supplier.

Common types of IT agreements

Note – consumer contracts under the Australian Consumer Law

Some IT agreements may also be consumer contracts or small business contracts under the Australian Consumer Law (**ACL**). If so, your organisation may have rights under consumer guarantee and Unfair Contract Terms provisions in the ACL, 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).

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

Make sure you are aware of these restrictions and that all your organisation's use of the software complies with these terms.

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.

Make sure the support services to be provided under the agreement are specified in sufficient detail and that response and resolution times are defined clearly.

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.

Also consider whether the supplier is required to make updates and new releases of the software available under the support agreement.

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.

Web hosting agreements

A web hosting agreement is likely to be relevant if your organisation has a website.

Under a web hosting agreement, the supplier provides the technology and services needed for a website to be visible on the internet. It may also supply other ancillary services to your organisation. These may include, for example, email services, domain name 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.

Consider:

- how those resources may be varied by the supplier under the agreement and the consequences of your organisation using excessive resources, and
- limiting the kinds of content you may publish on the website

Make sure the agreement allows your organisation to comply with its obligations under applicable privacy laws.

More 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 software and infrastructure 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.

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. Consider the location where the data will be stored, hosted or processed. If your data comprises personal or confidential information, it's recommended that the location is Australia or another jurisdiction with a strong privacy and data security regime be selected.

More information

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 ACL 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.

More information

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 purchase and maintenance agreements

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.

Consider when ownership and risk in respect of the hardware or equipment passes to your organisation, keeping in mind that ownership and risk may pass separately.

Agreements prepared by the supplier often provide that 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, so it's recommended your organisation obtain appropriate insurances. Also consider responsibilities with respect to delivery and unpacking of the hardware.

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.

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.

Also consider including milestones, which break the project down into measurable steps, in the agreement so that any issues can be resolved along the way. It may also be advisable to include testing requirements which the software must pass before it is accepted.

In a software development agreement, 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.

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.

More information

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

Key legal issues with IT agreements

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

More information

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.

What 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
- ✓ 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

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

Description of products or services ('specification')

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

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, or the supplier may have additional rights, which are not set out in the agreement itself.

It may not always be clear whether an external document actually 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, 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:

- ✓ If the supplier has such a right, 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 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 hold personal or sensitive information about their service users, employees or volunteers.

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

Support services often involve services being provided from outside of Australia.

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 (ie. 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
- ✓ 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

More information

See 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.

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
- ✓ 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

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.

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.

Tip

Certain statutory guarantees are set out in the Australian Consumer Law (**ACL**) 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 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)

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 ACL.

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
- ✓ Consider whether any limitation of liability in the IT agreement impacts your organisation's insurance

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

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 this is unlikely to be a large risk but it is still something you should consider.

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
- ✓ 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 may also include insurance may include professional indemnity insurance, public liability insurance, or workers' compensation insurance.

More information

See our guide to insurance and risk management for not-for-profit organisations.