



Handling confidential, market-sensitive information: Principles of good practice

Governance Institute of Australia

Governance Institute of Australia is the only independent professional association with a sole focus on the practice of governance. We provide the best education and support for practising chartered secretaries, governance advisers and risk managers to drive responsible performance in their organisations.

Without exception, our Members are all involved in governance, corporate administration and risk management. They have primary responsibility for developing and implementing frameworks in public listed and unlisted companies, as well as private companies, not-for-profit organisations and public sector agencies.

Our postgraduate education in applied corporate governance and risk management is unrivalled in its breadth and depth of coverage. It sets the standard for entry into the profession.

Postgraduate education is also the gateway to membership of Governance Institute of Australia and the Institute of Chartered Secretaries and Administrators (ICSA) — leading international associations for governance practitioners.

Our Certificates in Governance Practice, Governance and Risk Management and Governance for Not-for-Profits provide skills-based governance and risk management training, and a qualification for a wide range of professionals responsible for corporate accountability functions and processes within an organisation.

Australasian Investor Relations Association

The Australasian Investor Relations Association (AIRA) was established in 2001 to advance the awareness of and best practice in investor relations in Australia and New Zealand and thereby improve the relationship between listed entities and the investment community.

The Association's 165 corporate members now represent over A\$760 billion of market capitalisation or over two-thirds of the total market capitalisation of companies listed on ASX.

As the peak body for investor relations professionals within listed companies, AIRA promotes best practice and ethical and professional standards in investor relations, shareholder communications and corporate disclosure.

The Association offers an extensive program of investor relations professional development, learning and training activities to improve the skills and professionalism of its members, including the Diploma of Investor Relations, the Certificate of Investor Relations and a regular schedule of topical issue-based briefings and seminars.

These principles were revised in 2013 to take account of changes to Guidance Note 8 on continuous disclosure and have been further revised in 2014 to take account of matters raised by ASIC in its report *Handling of confidential information: Briefings and unannounced corporate transactions*.

Foreword

ASIC worked closely with Governance Institute of Australia (Governance Institute) and the Australasian Investor Relations Association (AIRA) on this guidance about the handling of confidential, market-sensitive information. It reflects our position on what good practice in this area entails.

ASIC sees the proper handling of confidential, market-sensitive information as fundamental to upholding the integrity of our financial markets. It empowers a company to manage the timely release of its information in accordance with continuous disclosure rules.

This guidance provides the direction that listed entities need when handling confidential, market-sensitive information. For this reason, ASIC welcomes and supports Governance Institute and AIRA's release of *Handling confidential, market-sensitive information: Principles of good practice*.

John Price
Commissioner
Australian Securities and Investments Commission

Introduction

Governance Institute and AIRA believe that adherence to the principles of continuous disclosure by listed entities is integral to the integrity and proper functioning of our equity markets.

Confidence in the integrity of Australia's markets could be undermined if investors believe rumours are actively spread in the market to distort proper price discovery.

It is therefore essential that corporations develop and adopt sound practices that support and adhere to the principles of continuous disclosure, ensure the effective management of confidential information and facilitate the responsible handling of rumours.

Governance Institute and AIRA have jointly developed principles of good practice that corporations can implement, taking into account the nature, size and

sensitivity of any particular transaction and the circumstances of the corporation.

Governance Institute and AIRA believe that the guidance set out in these principles will provide a strong foundation for improving practices for the handling of confidential information.

The principles are applicable in the context of capital raisings and mergers and acquisitions, and other transactions which corporations may undertake. They are designed to assist corporations and their advisers to implement robust policies and procedures to maximise the protection of confidential, market-sensitive information. In turn, this will ensure that corporations can manage the timely release of information in accordance with the continuous disclosure rules.



Tim Sheehy
Chief Executive
Governance Institute of Australia



Ian Matheson
Chief Executive
Australasian Investor Relations Association

Handling confidential, market-sensitive information: Principles of good practice

It is considered good governance for companies to establish policies and procedures to maximise the protection of confidential, market-sensitive information. Reducing the risk of leaks or insider trading promotes and preserves market integrity.

The *Corporations Act 2001* prohibits a person with market-sensitive information from trading or procuring trading by someone else or communicating the information to someone likely to trade or procure trading. The board, senior executives and other internal or external persons, who during a confidential, market-sensitive transaction have access to inside information relating directly or indirectly to the entity, need to understand clearly their obligations to protect this information and maintain its confidentiality where it is premature to disclose such information; for example, because it concerns an incomplete proposal or negotiation or is insufficiently definite to warrant disclosure.

ASX Listing Rule 3.1¹ requires immediate disclosure of market-sensitive information if it has ceased to be confidential. This obligation relates only to information that is market-sensitive, and not to all information held by an entity. These guidelines set out measures that can be considered when designing and implementing the policies and procedures that protect confidential, market-sensitive information, which is likely to be handled by a number of people within an entity as well as external parties.

The measures that any particular company may take will depend on its circumstances, the nature, size and sensitivity of any particular transaction, and the nature and timing of the transaction. On this basis, the guidance provided should be applied flexibly. It is up to the company to determine which measures are most applicable to each particular

transaction, within an overarching context of focusing the attention of all those who are party to a transaction on ensuring that they keep the market informed, on a timely basis, and maintaining confidence in market integrity.

The five principles of good practice that companies should adopt to maximise the protection of confidential, market-sensitive information are set out below.

Summary of principles of good practice

- 1 It is good practice for companies to have in place internal systems to protect confidential, market-sensitive information.
- 2 It is good practice for companies to maintain an insider list when conducting a confidential, market-sensitive transaction.
- 3 It is good practice for companies that deal with confidential, market-sensitive information to ensure their directors, executives and employees are aware of their confidentiality obligations.
- 4 It is good practice for companies to bind their advisers and other service providers by entering into confidentiality agreements before passing on confidential, market-sensitive information, and to require confirmation from their advisers and other service providers that they have in place policies and practices relating to the handling and control of confidential, market-sensitive information that satisfy the terms of the agreement.
- 5 It is desirable for companies to know which, when and how potential investors are being sounded on their behalf in relation to a transaction involving the company.

¹ Reference should be made to ASX Listing Rules Guidance Note 8: Continuous Disclosure — Listing Rules 3.1 – 3.1B in relation to the requirement to disclose confidential information should confidentiality not be maintained.

Internal policies: Protection of confidential, market-sensitive information

Principle 1: It is good practice for companies to have in place internal systems to protect confidential, market-sensitive information

A clear, documented policy which establishes the standards of behaviour and procedures for handling confidential, market-sensitive information with which all employees are expected to comply will assist a company to protect that information.

It is good practice to assign clear responsibility within the company to an individual to oversee the implementation and enforcement of these policies and controls, as well as regular reviews of how the policies are working in practice. This in turn will help to ensure they are being implemented effectively.

Companies that are most successful at protecting confidential, market-sensitive information embed practices for protecting that information in the culture of their company and reinforce these through regular messages from top management. Individuals need to be aware of their personal obligations to preserve the confidentiality of company information and the purpose of various systems that are used to protect confidential, market-sensitive information.

Any policy on protecting confidential, market-sensitive information must be consistent with the company's communication policy and if the company is a disclosing entity, its disclosure policy.

The 'need to know' principle

It is good practice to limit the number of people with access to confidential, market-sensitive information to the minimum number possible in the circumstances. That is, consideration needs to be given to how a company can limit access to information to only those people who absolutely require the information to undertake their business role.

Physical document management and information barriers

Taking particular care with documents relating to a proposed transaction can assist in minimising the leakage of confidential, market-sensitive information.

Companies should consider implementing the following practices:

- ensuring that employees who have access to confidential, market-sensitive information are aware of its status — the information should be marked as confidential and market-sensitive where appropriate
- ensuring physical copies of documents relating to confidential, market-sensitive transactions are securely stored when not in use and disposed of when no longer required, with access restricted to authorised staff only ('clean desk' policy)
- allocating dedicated printers, faxes, photocopiers, data rooms and other mechanisms for market-sensitive

transactions, where reasonably practicable and justified by the circumstances of the transaction. Ideally, these will be password-protected printers if used by other persons outside the team

- adopting appropriate code names for transactions to disguise the nature of and parties involved in the transaction
- regularly reminding staff not to read confidential, market-sensitive documents in public places (for example, airports, planes, cafes) or have confidential discussions in places where they could be overheard by others (for example, lifts, taxis), and
- ensuring that employees do not make unauthorised physical or electronic copies of confidential information and ensuring appropriate security measures are adopted where it is necessary for employees to remove or access physical or electronic copies of confidential information outside their workplace

Companies should also, when necessary, ensure that systems and controls are in place to quarantine confidential, market-sensitive information from contractors and other service providers that share access to the company's systems.

Consideration should be given to establishing discrete physical work areas for project teams if the project is likely to last for a significant period and involve large numbers of personnel. Off-site locations may be appropriate in some cases.

Information technology controls

It is important that information technology systems and practices are sufficiently secure to ensure that confidential, market-sensitive information is not inadvertently disclosed. The levels of security that a company will implement will depend on the sensitivity of the transaction and the nature of the company's information technology infrastructure, as there could be cost constraints for small companies.

Systems and practices that may help include:

- storing confidential, market-sensitive information on systems that implement logical access controls and only allow access to authorised personnel (external servers and cloud-based systems may need to be reviewed to ensure security of access is maintained)
- ensuring that all documents are password-protected from the outset
- providing separate passwords when transferring confidential, market-sensitive documents electronically. Also, such documents may be encrypted
- installing password-protection mechanisms for all electronic equipment (such as laptops, smartphones, tablets, USB drives and other storage media) containing

confidential, market-sensitive information or providing physical tokens for access that generate a new number each minute that can be provided via a smartphone, which replaces the password and ensures that directors, executives and external parties do not need to write down passwords which can be lost or stolen. Automatic locking should be activated after periods of inactivity on these devices

- installing appropriate software so that confidential, market-sensitive information held on a tablet or smartphone can be remotely deleted, to prevent unauthorised third party access should the tablet or smartphone be lost or stolen
- placing appropriate controls over staff access to other employees' electronic mail
- careful use of PINs for conference calls, for example, using a PIN for a conference call on market-sensitive transactions once only rather than using the same PIN multiple times, and dedicating such PINs to conference calls on market-sensitive transactions rather than using group PINs accessed for general purposes. The person chairing the call should make every effort to be aware of the security procedures available, to minimise the chance of inappropriate persons attending the conference call. This ensures that only the intended parties to the call can participate
- operating a document management system, depending on the size and resources of the company, that has the capacity to log who has accessed particular files and when the access occurred, and
- conducting regular reviews to ensure data storage and controls are up-to-date and secure.

Contact with external parties

Given that the media and other external parties are likely to actively contact people they believe have inside knowledge, a company's policies should explicitly cover contact with the media and other relevant external parties. The existence of a binding policy and appropriate training assists employees in dealing with these approaches.

Leak investigations

It is good practice for companies to have written policies and procedures on how a suspected leak of confidential, market-sensitive information is to be investigated, and employees should be made aware that such a process may be undertaken if there is a suspected leak. It is also good practice for companies to develop whistleblower policies that make it easy for employees to report instances of confidential, market-sensitive information being handled inappropriately.

Companies need to have in place procedures to announce confidential, market-sensitive information immediately, should such information be leaked and confidentiality is lost. A company could have a draft announcement prepared as a risk management measure in relation to such an eventuality.

If a leak of confidential, market-sensitive information occurs, the company needs to consider whether to undertake or instigate a leak investigation that may include requesting its advisers to undertake a leak investigation of their own. Whether an investigation should be undertaken, and the level of formality and intensity of that investigation, will depend on the significance and impact of the leak. A review process not only highlights any risk areas but also acts as a deterrent, raising awareness and signalling to employees that the matter is taken seriously.

Companies should develop clear guidelines as to when leaks, or the results of leak investigations, should be referred to external regulators or law enforcement agencies.

Legal advisers may need to be involved in the leak investigation in the event that there is a subsequent external investigation by a regulator such as the Australian Securities and Investments Commission (ASIC) or the Australian Prudential Regulatory Authority (APRA).

Reasonable person test

The disclosure obligations under Listing Rules 3.1, 3.1A and 3.1B require that: 'Once an entity becomes aware of any information concerning it that a reasonable person would expect to have a material effect on the price or value of an entity's securities, the entity must immediately tell the ASX that information'. Companies need to be aware of the 'reasonable person' test in relation to market-sensitive confidential information, which may apply regardless of whether relevant transactions have been completed.

Insider lists

Principle 2: It is good practice for companies to maintain an insider list when conducting a confidential, market-sensitive transaction

It is good practice for companies to maintain a register of both internal and external people (including directors and their staff) who are insiders on market-sensitive transactions, and efforts should be made to keep the number of these insiders to a minimum.

A company may arrange for some or all of its advisers and other service providers to maintain their own insider lists. Where such an arrangement is adopted, the company should ensure that the list maintained by the adviser or service provider will be made available to it immediately upon request.

Good practice is for companies to have a developed process for how and when people are brought 'inside' on sensitive transactions. It is appropriate for individuals to be reminded of their responsibilities each time they are made an insider.

It is also good practice for a company to implement a mechanism for removing from the insider list those people who are no longer involved in the transaction, as not all people remain insiders when the transaction takes place over a long period of time.

Unless advisers or other service providers are maintaining their own lists, they should provide the company with a list of the people within their firm who have been or will

be given access to the company's confidential, market-sensitive information on engagement, and then ensure the list is updated regularly. Lists need only be maintained until all the information about the transaction becomes public.

Insider lists should detail individually the people who are actively working on a transaction and indicate their role. People who are provided with confidential, market-sensitive information about a transaction on an ancillary basis — such as those acting in a compliance role or those who are providing word-processing, editing, IT or printing services — could be listed by category in circumstances where they might not be expected to see the details of a proposal. Some management personnel not involved in the transaction may also be covered by this principle.

Confidential, market-sensitive information should only be provided to those authorised to receive it. Company insiders should be made aware of the person to contact, should they need to know who else is on the insider list, including those from external advisory firms and other service providers who have been given access to confidential, market-sensitive information in relation to a transaction.

If an external adviser or other service provider needs to outsource a service in circumstances where confidential, market-sensitive information may be disclosed, it is good practice for the company to ensure the adviser or service provider first seeks the company's consent and ensures insider lists are maintained by that third party.

Internal policies: Individual confidentiality obligations

Principle 3: It is good practice for companies that deal with confidential, market-sensitive information to ensure their directors, executives and employees are aware of their confidentiality obligations

Employment contracts

Appropriate confidentiality obligations and securities trading restrictions should be incorporated into employment contracts and directors' appointment letters (by way of reference to the company trading policy for public listed companies) or other arrangements with all staff (including temporary employees) who may have access to the company's confidential, market-sensitive information.

To ensure that a company can actively monitor any potential insider trading, employment contracts should also explicitly include the employer's right to access all communication records, including corporate email and phone records. An employee's confidentiality obligations should survive beyond the termination of their employment.

Staff training

It is good practice to support policies dealing with confidentiality obligations with regular training programs and internal communications, as well as covering these matters in induction programs for new employees who might handle such information in their position.

It is recommended that staff undergo training on the importance of not improperly or inadvertently divulging confidential information, with particular focus on employees with access to market-sensitive information.

Staff should be made fully aware of the implications of improper disclosure of confidential, market-sensitive information and insider trading, and the potential civil and criminal liabilities for both an individual and the company.

Exiting employees

When employees who have access to confidential, market-sensitive information leave a company, it is good practice to conduct an exit interview with them. This provides an opportunity for the company to secure the return of confidential information from the exiting employee and remind them of their ongoing responsibility to maintain the confidentiality of inside information. It may be appropriate to require written acknowledgement of this.

Securities dealing

Public listed companies are required to have a securities trading policy that covers directors and executives (key management personnel). It is good practice for the trading policy to extend to include all executives and employees on an insider list for any transaction.

In addition to complying with the ASX Listing Rules, the following are measures that can be considered to implement a sound framework in relation to securities trading while a company is engaged in a confidential, market-sensitive transaction:

- Trading restrictions should extend to securities in companies with which the company is engaging in market-sensitive transactions.
- Where there is a transaction underway and employees are in possession of confidential, market-sensitive information, a company should consider putting in place blackout periods restricting trading for those employees in its securities and the securities of other relevant entities.

Where companies are not subject to the ASX Listing Rules, it is good practice to develop and implement a securities trading policy applicable to directors, officers and employees on an insider list relevant to a transaction. Such a policy would restrict trading in the company's and/or other parties' securities by employees who have possession of confidential, market-sensitive information. The trading policy should address the legal prohibition on insider trading.

Internal policies: Confidentiality agreements

Principle 4: It is good practice for companies to bind their advisers and other service providers by entering into confidentiality agreements before passing on confidential, market-sensitive information and to require confirmation from their advisers and other service providers that they have in place policies and practices relating to the handling and control of confidential, market-sensitive information that satisfy the terms of the agreement

Initial discussions with potential advisers and possible investors

Depending on the type of transaction, some companies can speak to multiple potential advisers and/or possible investors about a proposed transaction. When engaging in these initial discussions, companies should:

- keep a record of which advisers and investors they have approached, and when
- have a short script about the importance of maintaining confidentiality to use at the start of the initial discussions, and
- depending on the nature of the discussions, consider whether it is appropriate to have a pro forma confidentiality agreement ready for use.

'Beauty parades'

When a company conducts a tendering process, often referred to as a 'beauty parade', to select advisers for a specific confidential, market-sensitive transaction, it involves a high degree of disclosure, including to parties that miss out on a role in the transaction and have no ongoing relationship with the company.

Before releasing any confidential, market-sensitive information to potential advisers during the tender process, companies should require them to sign confidentiality agreements. If investment banks are participating in the tender, the confidentiality agreement should include restrictions on the particular business units of the bank that are permitted access to the confidential, market-sensitive information.

Where possible, companies should keep the number of parties invited to tender to a minimum, taking into account the importance of competitive tension in selecting advisers.

Engaging advisers

Engaging advisers (such as investment banks, lawyers, accountants, tax advisers, specialist valuers, financial communications consultants and investor relations consultants) or other service providers (such as credit

rating agencies, trading banks, stock brokers, registries and printers) to assist with market-sensitive transactions will necessitate the disclosure of confidential, market-sensitive information to those advisers. Companies need to consider how to minimise the risk that confidential, market-sensitive information provided to an adviser or other service provider is inadvertently or deliberately misused.

All advisers should be required to sign confidentiality agreements for specific transactions (unless an umbrella agreement or some other engagement arrangement fully sets out the confidentiality arrangements applicable to the transaction or a fiduciary obligation applies).

These confidentiality agreements should be entered into as soon as possible once an adviser accepts a role in a specific transaction, and not delayed until the commercial terms of a transaction are finally negotiated. Among other things, these agreements should restrict an adviser's use of the company's confidential, market-sensitive information, including limiting the number of individuals within the adviser's business that are given access to the information. The agreements may also cover conflicts of interest.

Where an adviser has both private and public sides to its business or needs to manage conflicts of interest, for example, between different clients, companies need to be confident that the adviser has sufficiently robust systems and controls in place to mitigate the risk of the company's confidential, market-sensitive information leaking from the private to the public side or being used inappropriately within the firm.

It is good practice for the confidentiality agreements to confirm that the advisers and other service providers engaged by companies have in place the policies and practices relating to the handling and control of confidential, market-sensitive information that satisfy the terms of the agreement.

Umbrella agreements

Companies that are active participants in merger and acquisition transactions or capital raisings and use the services of investment banks and other advisers on a regular basis may consider setting up umbrella agreements. These types of arrangements set out in advance the general principles and practices an adviser must adhere to when undertaking work for the company.

Specific transactions may require additional side agreements, which would be negotiated at the time of the transaction, but all general principles, including how third parties are to handle confidential, market-sensitive information, would be set out in the general umbrella agreement.

Specific terms relating to confidentiality that an umbrella agreement might incorporate include:

- requiring advisers to:
 - comply with the 'need-to-know' principle in relation to all confidential, market-sensitive information provided to them by the company, thereby restricting the people in the adviser's firm to whom the confidential, market-sensitive information can be disclosed
 - keep all documents and information belonging to the company in a safe and secure manner and if such action is consistent with legal obligations, promptly return or destroy such material at the company's request
 - at the company's request, establish and maintain an insider list in relation to any matter on which the company has instructed the adviser
 - conduct and report on any leak investigation requested by the company, and

- have in place appropriate IT systems and controls, including in relation to external servers, cloud-based systems, laptops, smartphones, tablets, USB drives and other storage media; and

- prohibiting advisers from:
 - publicly disclosing they are acting for the company without prior approval from the company, and
 - speaking to third parties in relation to the company without specific prior approval from the company.

Companies can also give consideration to how their information may be used by other divisions of a service provider, and consider restricting how it may be divulged by the provider in an umbrella agreement (for example, the credit division of a trading bank not advising the capital markets division).

Sounding the market

Principle 5: It is desirable for companies to know which, when and how potential investors are being sounded on their behalf in relation to a transaction involving the company

Sometimes it is important to obtain direct market feedback from potential or existing investors about a transaction, depending on the company's circumstances and on market conditions in general. However, it is important that, when the company is involved in the process, the confidentiality of market-sensitive information is maximised when taking a sounding on capital raisings or merger and acquisition proposals and formal procedures are adopted to ensure there is no breach of continuous disclosure or insider trading laws.

Companies should have a good understanding of the process that their banks or advisers intend to undertake if they sound the market in relation to a potential capital raising or other transaction.

There are significant risks attached to delegating responsibility for decisions about the conduct of soundings to advisers without understanding and requesting details of the process the adviser intends to use. The more extensive the potential soundings, the greater the risk of reduced control if such an understanding is not acquired.

In order to arrive at this understanding, it is useful to request details of the actual process including:

- the specific investors the bank or adviser intends to approach and whether the investors have appropriate controls for protecting confidential, market-sensitive information and not using it to trade until it is generally available
- the timing of any approaches
- the proposed limit on the time that information will be available to potential investors, and
- the intended number of potential investors, with a view to keeping it to the smallest number possible
- consideration of whether there is a need for a cleansing statement to be issued.

The company should carefully consider the adviser's proposed approach to soundings and should seek to limit soundings to as few investors as reasonably necessary to gain the relevant level of comfort or commitment.

Companies should ensure that soundings are conducted as close as possible to the proposed announcement of the transaction. Ideally, soundings should be conducted after the market has closed on the day prior to the proposed announcement. Trading halts may be used by companies to manage their continuous disclosure obligations.

Appendix A

Checklist for companies when engaging advisers who will handle confidential, market-sensitive information

Advisers who regularly deal with confidential, market-sensitive information relating to transactions from a range of parties should have comprehensive and restrictive controls over personal trading in financial products by their directors and employees. The scope of these practices and procedures will depend on the specific circumstances of the advisory firm and its activities.

It is good practice for companies engaging such advisers to enquire whether the adviser:

- maintains lists of restricted entities. Among other things, these lists should ordinarily cover:
 - entities the firm is currently advising or acting on behalf of, and
 - entities about which the firm has confidential, market-sensitive information
- requires pre-clearance of all securities trading.

In addition, further controls may be appropriate for investment banks and financial advisers. Therefore, it is good practice for companies engaging such advisers to

enquire as to whether the adviser's securities trading policy requires employees who may receive confidential, market-sensitive information to:

- disclose, on joining the firm, all their investments in financial products (both listed and unlisted)
- disclose, on joining the firm, all brokerage and trading accounts they control or in which they have an interest
- trade through an approved broker, and where that broker is not the firm itself, authorise the firm to receive copies of all contract notes or records of trade directly from the employee's broker, and
- impose, depending on the particular business area of the adviser, additional restrictions on trading including:
 - minimum holding periods, and
 - prohibitions on trading in financial products of issuers in particular industry sectors or competitors of particular clients.

It can also be useful for companies to enquire of their advisers if they have implemented an IT compliance system that tracks, audits and oversees employees' securities transactions.

Governance Institute of Australia

National office

Level 10, 5 Hunter St Sydney NSW 2000

T: (02) 9223 5744 **F:** (02) 9232 7174

E: info@governanceinstitute.com.au

W: www.governanceinstitute.com.au

Australasian Investor Relations Association

Level 12, 37 Bligh St Sydney NSW 2000

GPO Box 1365 Sydney NSW 2001

T: (02) 9872 9100 **F:** (08) 9872 9200

E: administration@aira.org.au

W: www.aira.org.au