OCTOBER 2022

ICAC
INDEPENDENT COMMISSION AGAINST CORRUPTION
NEW SOUTH WALES

# Probity aspects of ethics walls: guidance for dealing with commercial activities and other complex scenarios

## Introduction – what is an ethics wall?

This publication provides advice on probity aspects of ethics walls. It contains useful information for both governance and operational managers dealing with complex scenarios involving procurement, business and entrepreneurial activities. Agencies should obtain their own legal advice where required.

An ethics wall can be defined as **a structured information barrier that prevents the flow of restricted information between one group and another.**

Traditionally, ethics walls have helped provide a safeguard against legal problems arising from situations such as conflicting business operations. However, they are also used to address other probity concerns. Ethics walls have also been referred to as *information barriers, cones of silence, Chinese walls* and *ethical screens*.

Having an ethics wall does not imply that the ethics of people either within or outside the wall are questionable. It simply addresses transparency and risk management requirements. In some circumstances the absence of a properly functioning ethics wall may be conducive to corrupt or improper practices.

A formal ethics wall is often a better solution than ad hoc barriers to prevent information flows. A formal ethics wall is likely to be more comprehensive, rigorous and have a greater effect on organisational culture and internal communications patterns. It enables the agency to show external parties such as regulators, tribunals, the media and the public that it was thorough in its efforts to protect information and prevent abuse.

Where an ethics wall is appropriate it should be implemented as early as practicable. If it is not implemented, for example before the information requiring restriction is received, the agency may be unable to demonstrate that the information did not spread before adequate barriers were erected. The onus is typically on the agency to show that the steps taken to establish and maintain an ethics wall are adequate to ensure protection of restricted information.

An ethics wall requires more than just written policies and procedures; it requires a thorough understanding of the relevant procedures by all affected staff, and a willingness and ability to apply them.

## Kinds of ethics walls

There are two main kinds of ethics walls:

1) **where there are two groups limiting the information flows to each other**; for example, a division that engages in land regulation and a division that invests in property, typically with incompatible objectives

2) **where there is one group limiting the information flow to anyone outside of the group**; for example, a division investigating serious safety breaches.

Staff should only work on one side of the wall in situations where there are two groups restricting information flows to each other.

In most situations, walled off individuals can be permitted to work on non-related matters subject to the rules of the wall. Sometimes a walled off individual can be prevented from doing any work outside the wall and interactions with outside parties are strictly limited. This is because there is a danger with them working with people from the other side of the wall.

Generally, a wall is put around information, however, it can also be placed elsewhere. This could be, for example, around a person in a conflict of interest situation. Where an ethics wall is used in a conflict of interest situation the wall does not eliminate the conflict of interest; rather, it is only a technique for managing the conflict, which continues to exist.[1]

This publication focuses on a formal ethics wall. However, the guidance set out below may be of general assistance in situations where an agency needs to address the risk that information is misused. For example, when recruiting new staff, it is important that no one receives advance notice of the interview questions, which can be a significant risk if there are internal applicants. In most cases, this risk can be controlled without a formal ethics wall.

## Examples of ethics walls

The following table provides examples of ethics walls, through a number of situations, reasons for the ethics wall, and how it could be structured.

## Why do we have ethics walls?

Ethics walls reduce the opportunity for people inside the wall to:

- intentionally access, use or disclose restricted information inappropriately
- inadvertently disclose information to people who are not entitled to it
- let security of information partially or substantially lapse so that people who are not entitled to the information access it
- be involved in corrupt or other unacceptable uses of information.

Ethics walls also:

- reduce the likelihood of people outside the wall improperly accessing and using restricted information
- protect the reputations of the agency, people within the wall and entities outside of the wall

| Situation | Reason for the ethics wall | Structure of the ethics wall |
|---|---|---|
| An agency provides services to the public that compete with companies or other entities that it also regulates | The regulated entities may be concerned that the commercial part of the agency could gain competitive information from them and use it to compete unfairly | An ethics wall is constructed between the regulatory and commercial parts of the agency |
| An agency regulates, investigates or inspects a company for which some of its team formerly worked | There may be a concern that the relevant staff may:<br>• unfairly favour or disadvantage their former company, or<br>• misuse information that they gained while at their former company | Staff who formerly worked at the company are walled off from regulatory activities involving their former employer |
| A senior manager has a conflict of interest in relation to a project | There may be concerns the manager could favour their personal interest | The manager and the project team are walled off from each other |
| A regulator owns or co-owns a special purpose venture entity that provides services on a commercial basis to entities covered by the regulator | There may be concerns that the regulator will be softer in its regulation of entities that pay for services from its venture entity | Walls are established between the special purpose venture entity and the regulator for certain categories of information |
| A contractor provides services to an agency but also has other clients that deal with the agency | There may be concerns that the contractor or its employees could give the agency's information to its other clients | Walls are established within the contractor between:<br>• the employees working for the agency with access to the information<br>• the other employees of the contractor |

[1] As ethics walls may be put in place to help manage conflicts of interest, readers may find it useful to refer to the Commission publication *Managing conflicts of interest in the NSW public sector*.

- improve transparency and thereby increase trust for all parties
- reduce potential financial costs associated with suspicions, including litigation, appeals, audits and investigations.

## When should ethics walls be used?

It is always important to remember that information is at greater risk of being corruptly or improperly used if it is not adequately protected.

Ethics walls may be useful when it is important to:

- maintain confidentiality
- manage conflicts of interest
- control conflicts of duties within a government agency
- address apprehension of prejudice or bias
- demonstrate accountability
- ensure fair treatment
- minimise opportunities to profit from market sensitive information.

## Factors to consider

The factors that might affect an agency's need for an ethics wall include the:

- importance of the project or activity
- extent of potential reputational damage, financial losses and regulatory intervention if information is not restricted
- previous history of information or probity breaches
- ethical standards of an industry
- level of information sharing and networking within an industry
- value of the information
- ability of entities outside the ethics wall to make improper use of the information
- expectations of key stakeholders that information should be restricted.

### Case study – dealing with an incumbent contractor during a tender process

In its *Investigation into the over-payment of public funds by the University of Sydney for security services* report published in 2020 (Operation Gerda), the Commission found staff from security companies dishonestly obtained a financial benefit from a university while providing patrol guarding services. The staff created false entries on daily time sheets and submitted these for payment to the university. One of the security companies had been an incumbent contractor and was successfully awarded a new contract in 2015.

A senior executive at the university provided evidence that he was concerned about the informality between the security company's managers and the university's own staff; for example, meetings were held between in-house staff and representatives of the security company at the university's poolside café. In part, this situation arose because of the close physical proximity between contracted staff and university staff who sat together in an open-plan office. The embedding of security contractors at the university was a deliberate contract management strategy that was endorsed by the university.

During the security services tender, there was no record of the university taking measures, such as establishing ethics walls, to ensure the incumbent contractor did not access information about the tender process. This was particularly concerning as the contractor's staff had access to one of the tender evaluation panel member's work locations. There was also a reasonable apprehension that the staff could have overheard conversations or seen documents that would provide an unfair advantage during the tender process, including confidential information about deliverables and pricing in the proposals of other tenderers, and information about the focus, deliberations and expectations of the tender evaluation panel.

A representative from the university subsequently acknowledged that all tender documents should have been locked down. The Commission recommended that the university establish ethics walls and/or other safeguards where there is a risk that someone connected to a tenderer could access confidential information about a tender process and tenderers' submissions.

# Elements of an ethics wall

The following elements should be considered when designing an ethics wall:

- assess past experience and risks
- select the categories of information and groups/individuals to be covered
- written instructions, undertakings and training
- separation
- necessary crossing of the wall and people above the wall
- recordkeeping and monitoring
- advice and breaches
- third party notification and consent
- what happens after the wall is removed?

These elements are considered in detail below.

## Assess past experience and risks

The risk of information breaches, and perceptions of information breaches, should be assessed so that the design of the ethics wall will be appropriate for the specific circumstances of the project or activity. An ethics wall that may be appropriate for one set of circumstances may not be optimal for another.

An example of a risk to be covered is working remotely. If people within an ethics wall will be working remotely, especially from home, an assessment of their work environment should be considered. This might include security of their work area and communications, information storage, data destruction and related matters. Consideration might also be given to people in an employee's home who may have access to their work areas or overhear communications, especially whether any of these other people are from a group from whom information is protected.

If the agency has had experience with ethics walls, any lessons learned should be considered to make sure that mistakes are not repeated, and prior successes can be replicated. The experience of other agencies and organisations with similar arrangements might also be considered.

The opportunities (otherwise known as positive risks which may produce beneficial outcomes) from increased transparency may also be assessed. For example, establishing an ethics wall around an inspections division may allow the agency to provide advice to the industry on how better to comply with regulatory requirements.

## Select the categories of information and groups/individuals to be covered

When designing a wall, it is critical to know the categories of information that require restriction. For example, the aspects of the relevant information that are commercial, relate to a conflict of interest or may cause damage to those entrusting us with their information. Knowing the categories of information to be covered helps in designing all aspects of the ethics wall.

It is important that the categories of information be defined with sufficient clarity. For example, there is a difference between information about a court case and information about a party to that particular case.

A list should be made of all the people who are within the wall. Identifying their functions and roles may enable a better understanding of the organisational and reporting structures. It might also help highlight potential issues to take into account in the design of the ethics wall. For example, it may be necessary to temporarily alter an employee's reporting lines or team structure to preserve the wall. If the list of people is not comprehensive it may not be practical to show that the restricted information was adequately protected at all times.

The list will also help ensure clarity over who is entitled to access and disclose information. It will make various elements of the ethics wall easier to apply. Examples include identifying the individuals who should be allowed access, who should be included in monitoring reports, who should provide written undertakings and so on.

If only certain categories of groups of people should be prevented from receiving the information, then those groups should be identified.

When planning for who should be kept behind a wall, the following categories of staff should be considered:

- secretarial or administrative staff (walled off staff may need their own administrative assistance)
- IT staff with high levels of system access (that is, helpdesk, system administrators or super-users)
- corporate or shared services staff dealing with issues such as recruitment and procurement
- staff who handle confidential executive, board and audit and risk committee papers
- cleaners, maintenance workers and staff making deliveries.

Staff with secondary employment or their own businesses should receive particular attention if the barrier is between the agency and other organisations. Further details about the secondary employment or business may need to be considered to ensure there are no unacceptable risks.

Particular attention should be paid to prevent staff from moving from one side of the wall to the other.

## Written instructions, undertakings and training

Protocols should be established and documented for the operation of the ethics wall.

Each person within the ethics wall should be given written instructions on the operation of the arrangement. Key aspects of relevant processes should be covered to enable compliance and reduce the potential for misunderstandings that could lead to information leaks. Among other things, the existence of the ethics wall might itself be something that needs to be kept confidential.

A signed, written undertaking may be required from people inside the ethics wall to abide by the procedures.

A similar undertaking may, on occasion, also be used for entities outside the wall to commit to:

- refraining from attempting to access the restricted information
- refraining from using restricted information if it comes into their possession
- immediately reporting any incidents of restricted information being offered to them or coming into their possession.

The undertakings reinforce the importance of compliance with the rules and may also be useful in the investigation of alleged breaches and subsequent action.

Where there is an ethics wall between two groups and they are required both to protect information in their group, and refrain from using information from the other group, the undertaking may cover both sets of duties.

It may be appropriate in some cases to remind people of the operation of the ethics walls through a variety of awareness-raising means. For example, if the ethics wall has a long duration, it may be appropriate to have periodic education sessions.

It may also be appropriate to review confidentiality agreements and employment terms to ensure that there is adequate protection of restricted information after employees cease employment with the agency.

### Contractors

Contractors, their staff and other individuals who are not permanent employees of an agency may need to work behind an ethics wall. In some situations, the objective of the wall is to prevent a contractor from conveying sensitive information to another part of their company.

These entities and individuals should generally be contractually bound to comply with the protocols of the ethics wall. In some situations, it also may be necessary to seek assurance from the contractor regarding the processes, systems and controls their company has in place to give effect to the ethics wall. For example, audit certificates may be required, including from independent auditors selected by the agency. Contracts should also contain appropriate “right to audit” clauses as well as clauses binding contractors to cooperate with investigations. Adequate professional indemnity insurance may also be required. In addition:

- relevant contracts, undertakings and probity deeds should be executed before access to restricted information is allowed
- the ethics wall should contemplate the potential for changes in staff
- if there are subcontractors involved in an arrangement, the relevant contractual obligations involved in the wall should flow down to them.

Where relevant, contractors and subcontractors should be bound to ensure confidentiality in perpetuity, even if they change employer.

## Separation

Consideration should be given to generally limiting interactions between people on either side of the wall. This might involve, for example, changing or re-allocating other duties of staff, changing team or group structures, separating support services, providing separate work facilities and limiting areas where employees from the two groups interact.

Generally, the greater the physical separation, the better. Examples of physical access controls include swipe cards, keypads, and biometric security measures (such as facial recognition and/or fingerprints) that enable lift, floor, and room access.

Physically separating groups also reduces the risk of people overhearing conversations about restricted information and viewing restricted documents or screens. It also reduces opportunities for inappropriate discussions and mitigates other risks of information flows that breach the wall.

The physical separation of staff might involve secure rooms for telephone conversations and meetings. Ideally, in the case of high-risk projects, consideration might be given to separate kitchens, amenities and other common areas. Placing groups on separate floors or buildings might also be desirable. If this is not practical, placing other branches between the groups might be considered.

Additionally, the storage of physical files in secure areas that can only be accessed by relevant staff supports the retention of information within a wall.

It is also easy to forget that shared areas in a building are outside of an ethics wall, including locations such as corridors, lifts, foyers and hot desks. When in these areas, as well as public areas, people from inside the wall should be reminded to refrain from discussing restricted information with each other, having telephone conversations about this information, reading documents or using monitors and screens on which restricted information may be visible to others.

Agencies can separate the IT activities of teams in several ways. Some approaches include establishing email group distribution lists, creating team folders, saving information on dedicated servers and ensuring access is restricted to team members. In addition to routine IT security controls, there are some software packages available that are specifically designed to build and maintain ethics walls. This software can also facilitate conflict of interest checks and, pending the outcome of the check, identify relevant files for restriction to certain persons or teams.

It is important to establish information security protocols to provide clarity on how confidential information is to be separated and retained within a wall. As a general principle, information should be shared on a need-to-know basis. Such security protocols may include, but are not limited to:

- assigning appropriate security classifications to emails and physical and electronic files to show that they are restricted
- sending highly sensitive emails via encryption
- holding confidential discussions in contained meeting rooms or secure online meeting software rather than in open spaces
- always accompanying clients around the office and conducting meetings with clients in designated rooms located outside the general work area
- ensuring employees are only able to print after they have swiped their personal access card
- locking computers when leaving a workstation
- maintaining a "clean desk policy"
- assigning code names for projects
- using document headings or watermarks to identify that documents are restricted
- limiting the ability to download restricted information to removable storage
- prohibiting people from facilitating accesses for colleagues or at least including a requirement to disclose if this occurs
- having shredders or secure bins for disposal of documents.

Information protocols can be introduced to protect information that is not to be shared with or made available to those outside the wall. Controls to prevent misdirected emails, for example, include:

- disabling the autocomplete function so that an email address does not automatically populate to the "To" field, which requires employees to type in a full email address
- introducing a delay feature so emails are held for a period after hitting send but before being released
- using email checking software to recognise "high-risk" emails (for example, those outside the wall)
- employing pop-up messages notifying employees that an email is designated for external distribution.

Wherever feasible, the audit logs of relevant IT applications should be monitored, or at least made available for examination.

## Necessary crossing of the wall and people above the wall

There should be carefully defined procedures for dealing with situations where crossing an ethics wall may be permitted, including when a staff member is placed inside the wall on a temporary basis or requires a specific type of information that is restricted by the wall. The procedures may include:

- who may request permission
- the circumstances in which a request may be made
- how the request should be made
- documenting the request, including reasons for crossing the wall
- who makes the decision
- what should be assessed when considering the request
- documenting the decision as well as the reasons for it
- undertakings that may be required from the recipient of the information
- any markings to be placed on documents transferred and any relevant special security measures
- a register of all requests and decisions.

On occasion, managers will have responsibility for activity on both sides of a wall. This is often the case for the head of the agency and other senior managers with broad areas of responsibility. Despite the likely need for these individuals to have knowledge of activities on both sides of an ethics wall, agencies can still take steps to enhance probity. These include:

- avoiding targets and remuneration structures that could give managers an incentive to breach the ethics wall

- limiting the role of managers where it is practical do to so
- minimising the flow of information, including by removing unnecessary detail and de-identifying material where possible
- monitoring the conduct of managers (by the "ethics wall compliance manager", mentioned below) and including management in the scope of any audits
- ensuring that written protocols and associated training cover the roles of the managers.

## Recordkeeping and monitoring

Key aspects of an ethics wall should be documented, including key decisions, for transparency and accountability.

Ethics walls are generally important and would usually warrant the endorsement of senior management.

Additionally, it is better practice to appoint an ethics wall compliance manager to directly oversee the operation of the ethics wall.

Monitoring the effectiveness of the wall would typically include:

- reviewing alerts, security incident reports and exception reports
- ensuring that appropriate audits are performed
- reviewing audit/management reports, including of access to restricted information. The list of items to include in reports would depend on the type of information that is being protected, who has legitimate access, what their tasks are and so on
- reviewing key performance indicators
- checking that the protocols and ethics wall requirements are operating properly. Examples include all relevant people having signed required undertakings and received training, access restrictions being in place and access codes being changed regularly
- reviewing the performance and assurance frameworks of contractors and subcontractors
- requiring relevant staff to complete attestations at the end of the process.

The compliance manager will generally undertake the above activities.

The compliance manager will typically also liaise with specialist units such as risk management, operational compliance and internal audit. The agency's audit and risk committee should also generally have a role in assuring proper compliance with the ethics wall.

### Monitoring information accesses

Using data to identify indicators of unauthorised access is helpful in monitoring the effectiveness of an ethics wall. An agency could review specific data in relation to access and attempted access:

- by people from outside the wall
- indicated by swipe cards used in apparent contravention of the access rules
- by people accessing information that does not appear to be relevant to their duties
- made at unusual times, such as when the office is closed
- made in an unusual manner, such as from a remote location when the person works only in the office
- that seem to be larger than is needed for defined tasks, such as large parts of databases
- that appear to be too frequent for the tasks undertaken
- that appear to be of too short a duration for the person to complete the task associated with the documents
- that appear to be especially sensitive, particularly in relation to a person's work duties
- in given periods that are significantly more frequent or greater in size than the person's peers
- that appear to be related to an item in the news, of gossip or some trending interest
- that produce attachments that are subsequently included in emails where this is not the normal practice
- that is made by people above the wall, particularly when they do not need detailed information
- that is made for colleagues, not the person with access.

## Advice and breaches

People affected by the ethics wall should be given a source for advice if they have any concerns or need further information. The source should be available for the entire time that the ethics wall exists.

Similarly, there should be a process in place for reporting any suspected breaches of the ethics wall and associated protocols. The disclosure should be to the ethics wall compliance manager if it originates from someone within the wall and preferably to someone neutral (such as a governance unit) if the report is from someone outside the wall. Having two separate areas for notification may enhance the separation of the information, however, if it is not practical, then all disclosures could be to the ethics wall compliance manager.

Steps should be taken to fix the "hole in the wall" and decide what should happen with the disclosed information. Mitigation measures could include a person outside the wall who has received protected information signing an undertaking not to use or disclose that information and having no further involvement with the project. If they have already signed such an undertaking as part of the agreement to comply with the wall, this may not be required again.

People outside the wall may be informed about what to do if they become aware of or suspect breaches.

Where there are breaches of the ethics walls procedures there generally should be an investigation and where wrongdoing is found, action may be taken. Disciplinary action may be appropriate for staff involved. Other action may be taken against individuals and entities involved, including through administrative action, under the contract and utilising litigation. It may be appropriate to involve integrity agencies and relevant regulators.

## Third party notification and consent

Transparency entails showing people that the agency has followed key probity principles. To be transparent it is usually appropriate to disclose to individuals and other entities that the agency has an ethics wall.

This should entail informing them of the existence of ethics walls before they entrust their information to your agency or incur costs related to the transaction or systems. For example, a tender pack should explain that an agency within the cluster will be submitting a tender proposal and that an ethics wall is being established.

In some circumstances the decision of the other party to continue with the transaction or process indicates their implicit consent to the provision of information or participation in a process or transaction. However, it is always better practice to obtain an express consent. This could include, for example, an acknowledgement in writing that the agency's duty of disclosure does not extend to information held within the ethics wall.

## What happens after the wall is removed?

In many situations, the need for strict confidentiality disappears after completion of the relevant project, transaction et cetera. At this point, the ethics wall can be dismantled and staff can return to their usual business.

However, there may be certain information that needs to be kept confidential on an ongoing basis. While it is usually impractical to leave an ethics wall in place for lengthy periods of time, agencies can take steps to maintain probity, such as:

- ensuring that relevant contracts, undertakings and deeds address ongoing conduct
- clearly communicating with each person about their ongoing duties
- ensuring that relevant IT access controls remain in place
- safely disposing of all surplus paperwork (that does not need to be saved) and cleaning walled off office areas.

# Further information

The Commission's corruption prevention staff are available to advise public officials about probity aspects of ethics walls. Telephone 02 8281 5999 or 1800 463 909, or email advice@icac.nsw.gov.au.

I·C·A·C

INDEPENDENT COMMISSION AGAINST CORRUPTION
NEW SOUTH WALES

9 am – 5 pm Monday to Friday

Level 7, 255 Elizabeth Street
Sydney NSW 2000 Australia

Postal Address: GPO Box 500
Sydney NSW 2001 Australia

**Phone:** 02 8281 5999
**Toll free:** 1800 463 909 (outside metropolitan Sydney)
**National Relay Service users:** ask for 02 8281 5999
**Fax:** 02 9264 5364

icac@icac.nsw.gov.au
www.icac.nsw.gov.au