

# Policy

## Fraud and Corruption Control System

March 2025

[www.ocg.nsw.gov.au](http://www.ocg.nsw.gov.au)

OFFICIAL

# Contents

1.	Purpose of this policy .....	3
2.	Definitions .....	3
3.	Policy Statement.....	4
4.	Application.....	4
<b>Fraud and Corruption Control System .....</b>		<b>5</b>
5.	Foundations.....	5
5.1	Roles and Accountabilities.....	5
5.2	Fraud and Corruption Awareness .....	7
5.2.1	Types of fraud and corruption.....	7
5.2.2	Staff training .....	8
5.2.3	Stakeholder and supplier awareness .....	8
5.3	Fraud and Corruption Risk Management.....	9
5.3.1	Fraud and Corruption Register .....	9
5.3.2	Fraud and Corruption Risk Assessment .....	10
5.3.3	Fraud and Corruption Health Check .....	10
5.3.4	Internal Audit .....	11
5.3.5	Information Security Management System.....	11
<b>6.</b>	<b>Prevention</b> .....	<b>12</b>
6.1	Ethical behaviour framework .....	12
6.2	Internal Controls .....	12
6.2.2	Third party management systems.....	13
6.3	Risk-based internal audit program.....	14
<b>7.</b>	<b>Detection</b> .....	<b>14</b>
7.1	Proactive measures for detection of fraud and corruption .....	14
7.2	Reporting fraud and corruption by a staff member .....	15
7.2.1	Protection against reprisals .....	15
7.3	Reporting suspected fraud and corruption by our stakeholders and suppliers .....	16
7.4	External reporting bodies.....	16
<b>8.</b>	<b>Response</b> .....	<b>16</b>
8.1	Preliminary assessment.....	16
8.2	Full investigation.....	17
8.3	Disciplinary standards.....	17
8.4	Legal action.....	17
8.5	Maintaining confidentiality.....	17

8.6	Making vexatious, frivolous or misleading allegations.....	18
8.7	Recording reports of fraud and corruption .....	18
8.8	Crisis management following a fraud or corruption event.....	18
8.9	Review of internal controls, systems and processes post-detection of fraud or corruption.....	18
9.	Relevant legislation and standards.....	18
10.	Review.....	19
	Policy metadata.....	20

# 1. Purpose of this policy

This policy sets out the Office of the Children’s Guardian’s (OCG) fraud and corruption control system (FCCS), which aims to:

- establish the organisation’s policy position and ethical framework
- establish clear roles and accountability structures for management of the FCCS and response to allegations of fraud and corruption
- raise awareness of fraud and corruption risks that could occur at the OCG
- provide the requirements and guidance necessary to effectively prevent, detect and respond to fraud and corruption events.

This policy is consistent with the Australian Standard (AS) on Fraud and Corruption Control (AS 8001:2021) and the TC18-02 NSW Fraud and Corruption Control Policy.

This policy should be read in conjunction with OCG’s Information Security Management System (ISMS) Information Security Policy, which is based on ISO/IEC 27001:2022.

# 2. Definitions

Table 1: Definitions

<b>Control</b>	A measure that is modifying risk. Controls include any process, policy, device, practice or other actions which modify risk. ( <i>AS 8001: 2021</i> )
<b>Corrupt Conduct</b>	Deliberate or intentional wrongdoing, not negligence or a mistake. While it takes many forms, corrupt conduct occurs when: <ul style="list-style-type: none"><li>• a public official<sup>1</sup> improperly uses, or tries to improperly use, the knowledge, power, or resources of their position for personal gain or the advantage of others</li><li>• a public official dishonestly exercises their official functions, or improperly exercises their official functions in a partial manner, breaches public trust or misuses information or material acquired during the course of their official functions</li><li>• a member of the public influences, or tries to influence, a public official to use their position in a way that affects the probity of the public official's exercise of functions</li><li>• a member of the public engages in conduct that could involve one of the matters set out in section 8(2A) of the <i>Independent Commission Against Corruption Act</i> where such conduct impairs, or could impair, public confidence in public administration.</li></ul> <i>(Independent Commission Against Corruption)</i>
<b>Corruption</b>	Dishonest activity in which a person associated with an organisation (for example director, executive, manager, employee, or contractor) acts contrary to the interests of the organisation and abuses their position of trust in order to achieve personal

<sup>1</sup> The term ‘public official’ is defined in section 14 of the PID Act.

	<p>advantage or advantage for another person or organisation. This can also involve corrupt conduct by the organisation, or a person purporting to act on behalf of and in the interests of the organisation, in order to secure some form of improper advantage for the organisation either directly or indirectly.</p> <p>While conduct must be dishonest for it to meet the definition of ‘corruption’, the conduct does not necessarily represent a breach of the law. (AS 8001: 2021)</p>
<b>Fraud</b>	<p>Dishonest activity causing actual or potential gain or loss to any person or organisation including theft of monies or other property by persons internal or external to the organisation or where deception is used at the time, immediately before or immediately following the activity. Property in this context also includes intellectual property and other intangibles such as information.</p> <p>Fraud also includes the deliberate falsification, concealment, destruction or use of falsified documentation used or intended for use for a normal business purpose or the improper use of information or position for personal financial benefit.</p> <p>While conduct must be dishonest for it to meet the definition of ‘fraud’, the conduct does not necessarily represent a breach of the law.</p> <p>The concept of fraud within the meaning of this policy can involve fraudulent conduct by internal or external parties targeting the organisation, or fraudulent or corrupt conduct by the organisation itself targeting external parties. (AS 8001: 2021)</p>

---

### 3. Policy Statement

Fraud and corruption have the potential to impede the delivery of our functions, impact the financial position of our organisation, breach public trust and cause damage to our reputation. Therefore, fraud and corruption control is an integral part of the OCG’s broader risk management approach.

The NSW community expects public officials to perform their duties with honesty and in the best interests of the public. The OCG has a zero-tolerance approach to corrupt conduct, fraudulent activities or maladministration. We will continue to promote a culture of honesty, transparency and integrity within our organisation and are committed to:

- minimising the opportunities for fraud and corrupt conduct to take place
- implementing a robust, risk-based approach to prevent fraudulent activities occurring
- detecting, investigating and disciplining fraud and corrupt conduct
- reporting fraud and corrupt conduct to the Independent Commission Against Corruption (ICAC), the NSW Ombudsman or other external parties where appropriate.

A breach of this policy may lead to disciplinary action including termination of employment or engagement. Individuals found to have committed an offence under any relevant legislation may also be subject to penalties as prescribed by the legislation, which can include criminal charges.

---

### 4. Application

This policy applies to all OCG officers and recognises the role that each person plays in preventing, detecting and responding to suspected fraud and corruption. ‘OCG officers’ refers to public officials associated with the OCG. This includes all senior executive and non-executive staff, as well as workers engaged through contingent labour arrangements. This policy also applies to OCG suppliers who are expected to have similar fraud and corruption controls in place, as prescribed in the [Business Ethics Statement](#).

# Fraud and Corruption Control System

The OCG's FCCS establishes the foundations for effective fraud and corruption control, and outlines the measures in place for prevention, early detection and effective response. The FCCS includes the key risk management activities and internal controls, responsibilities, timeframes for action and information on review mechanisms.

---

## 5. Foundations

### 5.1 Roles and Accountabilities

A successful fraud and corruption control framework is led by a committed and accountable executive. The OCG's executive and Audit and Risk Committee have a critical role to play in relation to fraud and corruption control. There are also a range of other internal functions within the OCG that have an important role to play in the prevention and identification of fraud, including our People and Culture, General Counsel, Finance and Records Management functions.

#### 5.1.1 Children's Guardian

- Demonstrates leadership and models OCG values.
- Drives and promotes OCG's zero-tolerance to fraud and corruption.
- Has ultimate responsibility for the fraud and corruption control framework and endorses the control activities within the OCG.
- Is authorised to receive and manage reports of fraud and corruption, and refer those reports to external bodies as required.

#### 5.1.2 Director Corporate Services

- Administers the Fraud and Corruption Control Policy and reviews every two years.
- Is authorised to receive reports of fraud and corruption and has a central role in dealing with reports made by staff.
- Assesses reports of fraud and corruption and refers them within the OCG when necessary.
- Works with the Director People and Culture regarding allegations of fraud and corruption when appropriate.
- Ensures that investigations are conducted thoroughly.
- Ensures external agencies, including the ICAC and NSW Police are advised about fraud and corruption committed by staff in accordance with legislation.

- Conducts a Fraud and Corruption Control Health Check every 12 months.
- Reviews and updates the Fraud Risk Assessment every two years.
- Provides an annual status report to the Executive Leadership Forum, and Audit and Risk Committee on the fraud and corruption assessment and details of any investigations conducted during the year.

### 5.1.3 Audit and Risk Committee

- Provides independent assistance to the Children’s Guardian by monitoring and providing advice on the adequacy of the fraud and corruption control framework and the processes, controls and systems in place to capture and effectively investigate fraud and corruption related matters.
- Periodically reviews the Fraud and Corruption Control Policy and other strategies and their implementation.

### 5.1.4 Executive Leadership Forum (ELF)

- Reviews and approves the Fraud and Corruption Control Policy, promotes it within the OCG and monitors its implementation.
- Role models ethical behaviours to all staff.
- Supports the Children’s Guardian and Director Corporate Services in delivering the fraud and corruption control framework and control activities.

### 5.1.5 Director People and Culture

- Supports the Director Corporate Services in managing reports of fraud and corruption when appropriate.
- Ensures the welfare of staff involved in an allegation of fraud or corruption and that any breaches of conduct and behaviour are properly managed within the disciplinary system.
- Ensures new employees complete induction training including reading, understanding, and signing of the *Code of Ethics and Conduct* and associated policies as part of the acceptance of employment and completing the e-learning on Fraud and Corruption Awareness and Prevention.

### 5.1.6 Manager, Strategy and Systems

- Develops and maintains the Information Security Management System (ISMS) Information Security Policies and Procedures.
- Monitors fraudulent threats and activities, and manages internal IT control systems to prevent, respond to and recover from cyber security incidents including theft of data through ransomware attacks, fraudulent transactions made through IT systems and failing to protect security of personal or sensitive information held by the OCG.
- Assists in the capture and analysis of digital evidence in the event of any investigation following a report of a fraud and corruption incident.
- Works closely with other agencies in the IT shared services model to manage financial system IT controls.

### 5.1.7 General Counsel

- Manages data breaches and reporting in line with the [OCG Data Breach Policy](#).
- Provides legal advice on any arising fraud and corruption including any legal action required to be taken.

### 5.1.8 Managers, Team Leaders and Supervisors

- Understand the types of fraud and corruption that could happen within their area of responsibility and ensure their staff are also aware.
- Ensure they are familiar with this policy and are aware of their responsibilities for managing fraud and corruption risks.

- Ensure internal controls are operating in their areas.
- Report known or suspected fraud and corruption to the Children’s Guardian or Director Corporate Services as soon as possible.

### 5.1.9 OCG staff

- Actively take part in training including mandatory e-learning on fraud and corruption to contribute to the prevention and appropriate management of suspected fraud and corruption.
- Report known or suspected fraud and corruption to the Children’s Guardian or Director Corporate Services, as soon as possible.
- Cooperate with all investigations that may take place.

## 5.2 Fraud and Corruption Awareness

### 5.2.1 Types of fraud and corruption

A key element of the fraud and corruption control framework is creating awareness about what activities are considered fraudulent or corrupt.

This policy covers both internal and external fraud and corruption. Some examples relevant to the OCG are outlined below<sup>2</sup>.

Table 2: Examples of fraud and corruption

<b>Internal fraud</b>	<p>Fraud where at least one perpetrator is employed by or has a close association with the OCG and has detailed internal knowledge of the OCG’s operations, systems and procedures. Examples include:</p> <ul style="list-style-type: none"> <li>• An OCG employee creates a fictitious invoice where no goods or services are provided.</li> <li>• Unauthorised use of an OCG credit card for personal purposes.</li> <li>• Theft of funds held in OCG’s bank account by employees or others connected to the OCG, through use of privileged system access.</li> <li>• Theft of intellectual property or other confidential information belonging to the OCG, with the intention of using the information for some form of personal gain.</li> </ul>
<b>External Fraud</b>	<p>Fraud where the perpetrator is not an employee and has no connection with the OCG. Examples include:</p> <ul style="list-style-type: none"> <li>• Personal information or agency data is accessed by a person external to the OCG during a cyber-attack.</li> <li>• False invoicing, involving a person with no connection to the OCG creating a fictitious invoice claiming payment for goods and services not delivered or exaggerating the goods delivered or services actually provided.</li> <li>• Unauthorised access to the OCG’s bank account and transfer to a fictitious bank account, often initiated by way of a ‘phishing’ or ‘spear-phishing’ malware distribution.</li> </ul>

<sup>2</sup> Source: Adapted from AS 8001: 2021

<b>Corruption</b>	<p>Corruption (other than bribery) that may impact the OCG can include:</p> <ul style="list-style-type: none"> <li>• Releasing confidential information for other than a proper business purpose.</li> <li>• Manipulation of a procurement process by favouring one tenderer over another or selectively providing information to some tenderers and not others (but in circumstances where there is no payment of a bribe or other benefit).</li> <li>• Collusive tendering (the act of multiple tenderers for a particular contract colluding in preparation for their bids).</li> <li>• Serious conflict of interest involving improper use of an employee's position (especially managers and senior executives) or access to information, to gain or seek to gain a benefit or advantage for themselves or any other person.</li> </ul>
-------------------	--

### 5.2.2 Staff training

Staff need to understand fraud and corruption is not tolerated and the consequences should it be detected. They need to be aware:

- what fraud and corruption are
- common types of fraud and corruption they may encounter
- their responsibilities, and
- how to report suspected fraud and corruption.

Staff have a responsibility to contribute to eliminating fraud and corruption.

All staff must undertake our e-learning Induction Program. This program includes training on Fraud and Corruption Awareness and Prevention, the OCG Code of Ethics and Conduct, and Gift and Benefits.

To ensure all staff are kept up to date and continue to be reminded of their responsibilities regarding fraud and corruption post-induction, the following approaches will be taken:

- All staff will be required to annually complete the Code of Ethics and Conduct mandatory training
- a continuous and ongoing cyber security awareness campaign activities such as Phishing (email) campaigns and Vishing (Phone) assessments to monitor cybercrime
- all role descriptions will include the capability of Acting with Integrity
- regular awareness raising initiatives are undertaken
- this policy is regularly reviewed, updated and promoted to staff.

Overall responsibility for the fraud and corruption training rests with:

- the OCG ELT for oversight, supported by regular reporting from Corporate Services People & Culture
- all employees for proactively taking part in the training supported by their line managers and senior executives.

### 5.2.3 Stakeholder and supplier awareness

We are committed to ensuring that our stakeholders and suppliers are aware of our commitment to ethical behaviour. We have a Business Ethics Statement that sets out our position on fraud and corruption and expected standards of behaviour in business relationships with external parties. The Business Ethics Statement is published on our website, along with the Fraud and Corruption Control Policy, Code of Ethics and Conduct and Gifts and Benefits Policy.

We will collate information relating to fraud control and any related statistics to support regular

reporting, including for the annual report.

### 5.3 Fraud and Corruption Risk Management

Fraud and corruption are business risks which could have detrimental impacts on the organisation’s operations, finances, information assets and reputation. All staff must be alert to the possibility of fraud within the OCG.

The OCG employs a range of activities to help manage fraud and control risks and applies the risk management process set out in AS ISO: 31000:2018 ‘Risk management – Guidelines’:

1. Communication and consultation
2. Scope, context and criteria
3. Risk assessment
4. Risk treatment
5. Monitoring and review
6. Recording and reporting

The following table outlines the risk management activities undertaken by the OCG as part of the fraud and corruption risk management process.

Table 3: Risk management activities

Risk Activity	Responsible	Action	Communication
<b>5.3.1 Fraud and Corruption Register</b>	Senior Executive Assistant and Director Corporate Services	<p>Record details of the risks requiring treatment, controls and mitigation strategies in place.</p> <p>Record any potential fraud and corruption risks identified by staff or external parties and any actions taken to mitigate risk.</p> <p>Record any reported fraud and corruption incidents, the actions taken to respond and lessons learned.</p> <p>The register will be reviewed annually as part of the health check.</p>	All staff encouraged to report any potential risks to their manager and Director Corporate Services, who will document in the risk register

<p><b>5.3.2 Fraud and Corruption Risk Assessment</b></p>	<p>Director Corporate Services with the ELF and Executive Office</p>	<p>Undertake an OCG-wide risk assessment every 2 years, or when there is a substantial change in the function, structure or activities of the OCG. Risk assessment involves an in-depth analysis to identify potential vulnerabilities and growing risks within the OCG where fraud and corruption may occur. The risk assessment will:</p> <ul style="list-style-type: none"> <li>○ Undertake a scan of the potential internal factors (for example financial transactions, employee behaviour) and external environment factors (for example technological, economic, social) which may facilitate a fraud and corruption threat</li> <li>○ Document the risks identified</li> <li>○ Assess the effectiveness of existing controls for each risk</li> <li>○ Assess the potential impact of each risk and its likelihood of occurring to determine the risk level (for example low to very high)</li> <li>○ Determine actions necessary to eliminate any gaps and develop targeted mitigation strategies for each risk with responsibilities and timeframes for action and reporting.</li> </ul> <p>Findings will be incorporated into any broader Enterprise Risk Management and ISMS reviews and Business Continuity Planning.</p>	<p>Results will inform any training to be updated and communication promoted to all staff via an internal news item.</p> <p>Results will be presented to the ELF and Audit and Risk Committee</p>
<p><b>5.3.3 Fraud and Corruption Health Check</b></p>	<p>Director Corporate Services with the ELF and Executive Office</p>	<p>Undertake a health check every 12 months, to evaluate the OCG's overall compliance and control practices in relation to fraud and corruption risks which may include financial controls, data security, employee behaviour or operational performance. The health check will provide an overview of the key risks identified and recommendations for improvement. Findings will be incorporated into any broader Enterprise Risk Management and ISMS reviews and Business Continuity Planning.</p>	<p>Results will inform any training to be updated and communication promoted to all staff via an internal news item.</p> <p>An annual update report will be provided to the ELF and Audit and Risk Committee</p>

<p><b>5.3.4 Internal Audit</b></p>	<p>Third Party Provider managed by the Director Corporate Services and working with the ELF</p>	<p>Internal Audits are undertaken at least annually by a third-party provider.</p> <p>Internal audits assist in deterring fraud and corruption by examining and evaluating the adequacy and effectiveness of internal controls. It is also expected that the internal audit will evaluate whether the senior management is appropriately overseeing the fraud and corruption control policies and practices in place.</p> <p>Internal audit is not responsible for detecting fraud and corruption but is expected to obtain assurance that any material control deficiencies are detected. Internal audit must report known or suspected fraud to the Children’s Guardian or Director Corporate Services if they detect it.</p>	<p>Internal Audit reports are shared with the ELF and Audit and Risk Committee</p> <p>The outcomes and any actions are shared with relevant staff for implementation</p>
<p><b>5.3.5 Information Security Management System</b></p>	<p>Manager Strategy and Systems</p>	<p>The Information Security Management System (ISMS) Policy, consistent with ISO/IEC 27001:2022, aims to minimise the impact of security incidents such as malicious and fraudulent attacks on the operations of the OCG.</p> <p>The ISMS Policy supports our interests by defining management requirements for safeguarding our information assets and assuring the continued delivery of services.</p> <p>The ISMS Policy is reviewed annually with the ELF.</p>	<p>The ISMS Policy is published on the intranet.</p>

---

## 6. Prevention

---

### 6.1 Ethical behaviour framework

The OCG has clear policies setting out acceptable standards of ethical behaviour that are made available on the intranet and [OCG's webpage](#), and should be read in conjunction with this policy:

- [Business Ethics Statement](#)
- [Code of Ethics and Conduct](#)
- [Conflicts of Interest Policy](#)
- [Data Breach Policy](#)
- [Gifts and Benefits Policy](#)
- [NSW Procurement Policy Framework](#)
- [Public Interest Disclosures Policy](#)
- [Records Management Policy](#)

Staff are required to annually evidence their commitment to acceptable standards of ethical behaviour. This is undertaken by reading and acknowledging their acceptance of the Code of Ethics and Conduct as part of our mandatory training, via the myCareer portal. Executive leaders and managers are responsible for ensuring that their staff have completed this mandatory training.

We are committed to employing staff who support our ethical values. Pre-employment screening is used to verify information supplied by candidates on their resumes and applications and includes two reference checks prior to a position being offered. A Working with Children Check and a criminal history check is also required prior to the start of employment.

All role descriptions at the OCG include the capability of Acting with Integrity and these capabilities are also measured against in the performance management cycle.

---

### 6.2 Internal Controls

There is a strong link between fraud and corruption events and poor internal control systems<sup>3</sup>. Therefore, it is essential that the OCG's internal control system is well documented, regularly updated and understood by all staff.

We implement and maintain appropriate prevention and detection controls to manage the target risks identified as part of the risk management process. We maintain appropriate controls including:

- segregation of duties and decision making
- approvals and authorisation processes
- financial delegations integrated into the SAP system
- financial delegation of an OCG officer who can commit or incur a general expenditure outlined in the OCG Financial Delegations fact sheet
- financial reconciliations
- workforce screening and verification of OCG suppliers
- management reviews
- data analytics and mining tools
- risk assessments
- physical security and asset management
- cyber security

---

<sup>3</sup> AS 8001-2021

- independent reviews like internal and external audits.

Pressure testing internal controls for risks with a high-risk rating (for example major information security breach) may occur to ensure controls are operating as intended. Lessons learned sessions following a fraud or corruption incident will also be held and documented, with controls updated accordingly to mitigate future risks.

Examples of control measures we use to mitigate and manage common types of fraud and corruption are listed below.

Table 4: Examples of OCG fraud and corruption controls

Fraud and corruption risk	Control measure
Procurement fraud: Manipulation of a procurement process by favouring one tenderer over another.	<ul style="list-style-type: none"> <li>• Procurement policies and procedures managed through third party (DCJ)</li> <li>• Verification of OCG suppliers</li> <li>• Financial delegations and authorisations</li> </ul>
Financial fraud: An OCG employee creates a fictitious invoice where no goods or services are provided.	<ul style="list-style-type: none"> <li>• Financial delegations and dual authorisations integrated into the SAP system</li> <li>• Reconciliations</li> <li>• Regular audits</li> </ul>
External fraud: Personal information or agency data is accessed by a person external to the OCG during a cyber-attack.	<ul style="list-style-type: none"> <li>• Information Security Management System policy and procedures in place</li> <li>• Continuous cyber security awareness campaign activities to all staff such as Phishing to monitor cybercrime</li> <li>• Regular software updates, use of firewalls, multi-factor authentication, regular back up of data, endpoint protection</li> <li>• Data analytics and mining tools</li> <li>• Risk assessments</li> <li>• Regular training and reminders</li> </ul>
External attempts to bribe OCG Officers for personal gain.	<ul style="list-style-type: none"> <li>• Code of Conduct for employees and Business Ethics Statement for suppliers provided and available on the intranet and internet.</li> <li>• eLearning for employees</li> <li>• Screening new employees and verification of suppliers</li> <li>• Gifts and benefits policy</li> </ul>

## 6.2.2 Third party management systems

We will ensure specific internal controls relating to third parties, such as segregation of duties, are in place to manage our dealings with third parties. We will provide a copy of our Statement of Business Ethics setting out our expected standards of behaviour and mutual obligations of all parties, to our stakeholders and suppliers.

We are committed to complying with PBD-2017-07 Conduct by suppliers (Procurement Board Direction) by ensuring that:

- our tendering processes require tenderers to comply with the relevant policies and procedures as listed in the direction and provide information concerning any findings of dishonest, unfair, unconscionable, corrupt or illegal conduct against the tenderer, its director or management, and
- we are aware of any adverse findings against a supplier and report such findings to the NSW Procurement Board when such findings become known to us.

Third party management also covers managing staff conflicts of interest. The Code of Ethics and Conduct, and Conflicts of Interest Policy, set out how staff should manage conflicts of interest, including secondary employment. All staff are required to complete a Conflicts of Interest Declaration should they become aware of a real or perceived conflict of interest. All secondary employment approvals must be reviewed and reapproved annually.

---

## 6.3 Risk-based internal audit program

We engage external providers to undertake internal audits to assess the effectiveness of our internal controls, examine risk and detect irregularities. We generally select, in consultation with the Executive Leadership Team, Chief Audit Executive, and Audit and Risk Committee, two to four areas (Operational or Corporate) to focus on. Internal audit recommendations are recorded and are followed up regularly, with responsibility assigned to individuals and clear timetables set for response. Outcomes of reviews are reported to the Executive Leadership Team and the Audit and Risk Committee. Management uses internal audit findings as an opportunity to improve systems and processes.

The Chief Audit Executive and Audit and Risk Committee regularly review the internal audit program.

In addition, as part of the outsourced shared services arrangements in place for certain OCG corporate services, the OCG regularly receives and assesses self-attestations from its providers. Annually, these self-attestations are assessed by an external provider appointed by the Department of Customer Service, currently Deloitte.

---

# 7. Detection

## 7.1 Proactive measures for detection of fraud and corruption

The OCG takes proactive measures to identify risk and detect fraud and corruption, including through:

- identification of early warning signs through regular review of internal controls and risk register
- conducting yearly health checks and an agency-wide risk assessment every two years
- information security measures to identify any risks of cyber attacks and technology enabled fraud, including regular cyber security awareness campaigns and training
- internal audits conducted by external providers
- post-transactional review, reconciliations and analysis of management accounting reports
- annual completion by all staff of the Code of Ethics and Conduct and other mandatory training
- encouraging staff to report suspected fraud and corruption and promotion of whistleblower protection

- review of customer feedback through various channels (phone, email, website) with an appropriate process in place for managing complaints and feedback
- implementing and reviewing staff exit surveys for the identification of any fraud and corruption risks or concerns.

---

## 7.2 Reporting fraud and corruption by a staff member

We require staff, and encourage our stakeholders and suppliers, to report known or suspected fraud and corruption or unethical behaviour.

Staff should be aware of the provisions in section 316(1) of the *Crimes Act 1900* which says that a failure to report a serious offence, including fraud, is an offence.

If a staff member knows or suspects another staff member has acted fraudulently or corruptly, they must report it to either the:

- Director Corporate Services or
- Aboriginal Assistant Guardian or
- Children’s Guardian.

Staff are encouraged to make a report in writing, as this helps to avoid any confusion or misinterpretation, but reports can be made orally.

In most instances, reports can be dealt with internally. However, if staff have concerns that their report of fraud or corruption will not be dealt with appropriately then they have the option of reporting directly to ICAC.

In addition to the above notification on fraud or corrupt allegations, a staff member can make a public interest disclosure to the NSW Ombudsman in respect of internal corrupt conduct, maladministration or serious and substantial waste of public money. For guidance on how to report, refer to the [Public Interest Disclosures Policy](#).

If staff suspect that another organisation or person is defrauding the OCG, the suspicion can be discussed with their manager in the first instance or directly with the Director Corporate Services or the Children’s Guardian.

### 7.2.1 Protection against reprisals

We will not tolerate any reprisal action against staff and will ensure appropriate action is taken to protect staff (‘whistleblowers’), who report suspected fraud and corruption.

If someone believes detrimental action is or is likely to be taken against them, or the internal reporter, they should tell:

- their manager
- Director People and Culture
- Director Corporate Services, or
- Children’s Guardian.

We will make sure that internal reporters are supported and encouraged to access the professional support service they may need as a result of being part of this process – such as stress management, counselling service or legal advice.

The [Public Interest Disclosures Policy](#) also provides information on what protections are available to employees in making a report of serious wrongdoing and how will a report be dealt with.

---

## 7.3 Reporting suspected fraud and corruption by our stakeholders and suppliers

Our stakeholders, suppliers and members of the public are encouraged to report suspected cases of fraud, misconduct or unethical behaviour by staff members of the OCG. Our [Complaints Management Policy and Procedures](#) outlines how to make reports.

Any substantial fraud or corruption should be referred to the relevant external body (see 7.5). Where, on reasonable grounds, there is suspicion that corrupt conduct has occurred, the Children's Guardian has a duty under section 11 of the *Independent Commission Against Corruption Act 1988* to report it to ICAC as soon as the suspicion arises. This is irrespective of how significant or minor the allegation.

---

## 7.4 External reporting bodies

- [Making a report of corruption to the Independent Commission Against Corruption \(ICAC\)](#)
- [Making a report of serious wrongdoing to the NSW Ombudsman](#)
- [Making a report of frauds and scams to NSW Police](#)
- [Making a report to the Audit Office of NSW](#)
- [Making a privacy complaint to the Information and Privacy Commission](#)

---

# 8. Response

## 8.1 Preliminary assessment

When an allegation of fraud or corruption is made against a member of staff (the alleged perpetrator) the Director Corporate Services, Director People and Culture and/or the Children's Guardian will discuss the matter with the internal reporter. The internal reporter may be asked to make a written statement regarding the allegations.

The alleged perpetrator may be interviewed during this preliminary stage and can be accompanied by their manager or other nominated staff member during the interview.

The Director Corporate Services:

- will acknowledge the report of fraud or corruption within ten working days of receipt (and no later than 45 days) providing the name and contact details of the people who can provide further updates or information
- will organise a preliminary assessment of the allegations and provide details to the internal reporter of any decisions and how the allegations will be progressed
- may, if the allegation is serious and the evidence is compelling, recommend to the Children's Guardian that the matter be immediately referred to an external body. A full investigation may still be undertaken even though another agency, such as the NSW Police Force or the ICAC, is also investigating.

---

## 8.2 Full investigation

Following the preliminary assessment, the Director Corporate Services may recommend to the Children's Guardian a full investigation by an appropriate qualified external investigator. Any internal investigation should be conducted in accordance with ICAC's '[Factfinder: a guide to conducting internal investigations](#)', where appropriate.

The internal reporter will be advised of the decisions and any actions that will be taken. When further action is to be taken, the alleged perpetrator may also be notified.

During the investigations disciplinary policies will be properly followed to ensure that any personnel issues affecting the staff members involved are fairly addressed.

Proper and full records will be kept during the investigation and any evidence gathered will be secured and preserved.

Where third parties are affected by the fraud or corruption event, the OCG may consider whether it is appropriate to notify these parties.

The safety of investigators will be taken into consideration, including assessing whether appropriate protocols, training and supports are in place during the course of the investigation.

---

## 8.3 Disciplinary standards

Where the allegation is proved because of an admission by the staff or because of an investigation, the Director Corporate Services will make a recommendation to the Children's Guardian regarding disciplinary action or referral to an external body. The Director People and Culture may also be consulted in this process.

The Children's Guardian will determine the nature of any disciplinary action.

---

## 8.4 Legal action

The OCG may be required to consider legal action for recovery of losses (including stolen funds or property). via civil, criminal, or administrative processes, where the benefits of such recovery are considered worthwhile.

---

## 8.5 Maintaining confidentiality

Every endeavour will be made to ensure that any allegations of fraud or corruption and subsequent investigations are handled confidentially. This is to help prevent any action being taken against internal reporters. However, there may be situations where confidentiality may not be possible or appropriate. This will be discussed with the internal reporter.

While anonymous reports are not encouraged, there may be situations where someone may not want to identify themselves. We will accept anonymous reports. However, anonymity may limit our ability to seek further information to assess the report adequately or report back to the internal reporter on any finding or decisions. When the identity of the internal reporter is known, we can obtain any further information, provide the person with protection and support and give feedback about the outcome of any investigation into the allegations.

---

## 8.6 Making vexatious, frivolous or misleading allegations

Any vexatious, frivolous or misleading report will result in disciplinary action being taken against the internal reporter.

---

## 8.7 Recording reports of fraud and corruption

The Director Corporate Services will maintain records of all reports of suspected fraud and corruption. The Children's Guardian and Director People and Culture are responsible for providing the Director Corporate Services with the details of all reports of suspected fraud and corruption. These records will help us to document decisions and decision-making criteria, as well as determine where to focus future efforts and where changes to controls, policies or procedures are required as part of continuous learning and improvement. These sensitive records will be handled in accordance with our relevant policies and procedures.

Where appropriate, instances of suspected fraud and corruption will be reported to ICAC, NSW Policy or other regulatory bodies as required.

De-identified information will also be provided for reporting to the Audit and Risk Committee and external regulatory bodies as required.

---

## 8.8 Crisis management following a fraud or corruption event

Some major fraud and corruption events may require crisis management where there has been major disruption to the business, particularly those that have significantly impacted the OCG's operations, finances, data holdings, reputation and staff morale.

The OCG's Business Continuity Plan includes protocols for internal and external communications and procedures to follow when a suspected case of fraud and corruption involves senior personnel.

---

## 8.9 Review of internal controls, systems and processes post-detection of fraud or corruption

Post-incident, the Director Corporate Services and other relevant staff and leadership team will reassess the adequacy of the internal control environment and consider where improvements could be made. The Audit and Risk Committee and internal audit function may also be involved in post-incident debriefing and providing recommendations for remedial action or enhancements to existing controls.

---

# 9. Relevant legislation and standards

### Legislation

- *Public Interest Disclosure Act 1994*
- *Independent Commission Against Corruption Act 1988*
- *Government Sector Finance Act 2018*

### Standards

- AS 8001-2021 Fraud and Corruption Control
- AS ISO 31000 Risk Management (Guidelines)

- AS ISO 37001 Anti-bribery management systems (Requirements with guidance for use)
- AS ISO / IEC 27001 Information Technology – Security Techniques - Information Management Security Systems (Requirements)

#### Useful resources

- [Treasury Circular TC 18-02 – NSW Fraud and Corruption Control Policy 2018](#)
  - [Audit Office - Fraud Control Improvement Kit 2015](#)
  - [ICAC – Factfinder: a guide to conducting internal investigations 2022](#)
- 

## 10. Review

This policy is reviewed every two years or earlier, if significant new information, risk factors legislative or organisations change warrants an update.

---

# Policy metadata

Table 5: Policy metadata

Category	Description
Status	Approved
Date of approval	26 March 2025
Approver	Executive Leadership Forum
Directorate	Corporate Services
Policy owner	Director Corporate Services
Document location	Internal and External Website
Next review date	March 2027
Superseded document	All previous versions of OCG Fraud and Corruption Control Policies
Document Reference	A9399778

---

## Office of the Children’s Guardian

[www.ocg.nsw.gov.au](http://www.ocg.nsw.gov.au)

Switchboard: (02) 8219 3600

Locked Bag 5100  
Strawberry Hills NSW 2012