Fraud and Corruption Control Guide

Contents

Background

MP 0105/19 *Fraud and Corruption Control Policy* (policy) sets the minimum requirements WA health entities must meet to prevent, detect and respond to fraud and corruption. The Fraud and Corruption Control Guide supports the practical application of the policy, in particular the development and implementation of the Fraud and Corruption Control System (FCC System).

1. Introduction

Fraud and corruption undermine the public's trust and confidence in the WA health system and may:

- cause financial harm and loss
- damage the culture within entities and across the WA health system
- compromise consumer care and safety
- impede the effective delivery of services.

Fraud and corruption controls are a critical part of good integrity governance systems. Good integrity governance is achieved by creating an environment of transparency in and accountability for, preventing, detecting and responding to fraud and corruption risks and integrity issues to enable a culture of integrity to develop.

1.1 Statement of entity attitude to fraud and corruption

The policy prescribes zero tolerance exists for fraud and corruption in the WA health system and fraud and corruption are serious offences which will be managed accordingly.

It is important entities acknowledge fraud and corruption as serious business risks and demonstrate a high level of commitment to establishing and maintaining a culture and integrity environment which controls the risk of fraud and corruption.

1.2 Link to entity's codes of behaviour

Not engaging in fraudulent and corrupt behaviour is one of the Principles of Conduct with which staff must comply under the WA health system Code of Conduct.

MP 0124/19 *Code of Conduct Policy* requires staff must:

- act ethically and not engage in conduct which is, or may be interpreted as, fraudulent or corrupt
- not engage in conduct which is dishonest or may cause harm to a person
- not engage in acts of minor or serious misconduct as defined in the *Corruption, Crime and Misconduct Act 2003* (WA) (CCM Act)
- familiarise themselves and act in accordance with their relevant discipline policy, the *Health Services Act 2016* (HS Act), *Public Sector Management Act 1994* (PSMA), CCM Act and relevant health professional codes of conduct.

2. Fraud and Corruption Control System

The FCC System is a comprehensive framework for addressing fraud and corruption risks aimed at reducing an entity's exposure to fraud and corruption. A FCC System is an integral part of overall risk management to address fraud and corruption business risks which are mitigated by the application of risk management controls.

The FCC System seeks to control:

- internal fraud and corruption against the entity and its operations
- external fraud and corruption against the entity and its operations
- fraud and corruption involving persons internal to the entity in collaboration with persons external to the entity
- fraud and corruption by the entity or by persons purporting to act on behalf of and in the interest of the entity
- fraud and corruption by business associates.

The policy prescribes the FCC System must align to the principles of Fraud and Corruption Control Australian Standard AS 8001:2021 (AS 8001:2021). To meet this requirement, the FCC System must consider all policy frameworks and existing local policies addressing fraud and corruption risk. This avoids duplication, inconsistency and uncertainty.

The policy prescribes entities must establish and implement a FCC System, which is endorsed by their governing body, within three months from the date of the policy coming into effect. The FCC System must be reviewed and evaluated at least every two years.

2.1 Roles and accountabilities

Clearly defined and communicated roles and accountabilities for controlling an entity's fraud and corruption exposures are essential to an effective FCC System.

Roles and accountabilities may vary between entities. Exemplar roles and accountabilities are provided in Table 1.

Table 1: Exemplar FCC System roles and accountabilities

Role	Accountabilities
Department of Health employees / health service provider Staff Members	Pursuant to the Code of Conduct, all staff must act professionally and ethically and demonstrate honesty and integrity. As well as being accountable for their own behaviour and decision making, staff must take responsibility to identify and report suspected fraudulent or corrupt behaviour.
Governing body	The governing body has overall accountability for ensuring the entity has in place adequate anti-fraud and anti-corruption measures, as part of its function to develop and monitor corporate governance arrangements. The governing body is responsible for setting the strategic direction for the entity and this includes maintaining, modelling and fostering the highest standards of ethical behaviour.

Role	Accountabilities
Audit and Risk Committee	The Audit and Risk Committee is responsible for the review and oversight of the internal audit function. This includes oversight of internal controls, risk management and fraud and corruption prevention. The Audit and Risk Committee provides advice, independent assurance and assistance to the governing body.
Chief Executive / Director General	The Chief Executive of a Health Service Provider (HSP) and the Director General for the Department of Health, have accountability for the day to day management of the entity and are responsible for providing leadership and direction in relation to integrity and ethical governance issues. The Chief Executive/Director General is responsible for the effective and economical use of resources, including coordinating resources in order to control the entity's fraud and corruption exposures. The Chief Executive/Director General is responsible for maintaining awareness of the entity's current fraud and corruption exposures and ensuring the development and implementation of the FCC System.
Fraud and Corruption Control Executive Sponsor	The Fraud and Corruption Control Executive Sponsor is responsible for: • championing fraud and corruption controls within the executive team and the broader entity • assisting with controls being effectively integrated into strategic planning, corporate governance and operational systems • overseeing the implementation and ongoing monitoring of the FCC System.
Executive Committee	The Executive Committee model ethical behaviour and are responsible for maintaining awareness of the entity's current fraud and corruption exposures. The Executive Committee provides leadership ensuring: • compliance in relation to the FCC System and the policy • controls are effectively integrated into strategic planning, corporate governance and operational systems • adequate resources are allocated to integrity and governance issues • support for a strong integrity and ethical culture as an essential and integral component across the entity.

Role	Accountabilities
Line Managers, including executives and senior managers	Line managers are accountable for fraud and corruption control within their business unit and are responsible for ensuring the FCC System is effectively implemented within their business units, in particular: • modelling ethical behaviour • providing leadership, guidance and support of staff in preventing, detecting and reporting suspected fraud and corruption • ensuring staff complete Accountable and Ethical Decision Making (AEDM) training and other relevant training and development activities • developing and modifying local work practices to reduce the risk of fraud and corruption • identifying and managing fraud and corruption risks in accordance with entity policy • receiving reports of suspected fraud or corruption from staff and taking appropriate steps in accordance with MP 0124/19 *Code of Conduct Policy* and entity policy • reporting suspected fraud and corruption promptly and maintaining confidentiality to ensure the protection of complainants who report fraudulent or corrupt activities. Line manager responsibility for preventing and detecting fraud and corruption is specified in relevant job descriptions and is incorporated into the performance management system.
Integrity Unit	The Integrity Unit delivers a specialist fraud and corruption control function. The Integrity Unit is responsible for: • developing, implementing and promoting the FCC System • collaborating with relevant others to ensure fraud and corruption risks are incorporated into the overall risk management system • developing and implementing fraud and corruption awareness and education programs • oversight of fraud and corruption events which involve staff, through their role in the ongoing oversight of disciplinary matters • ensuring appropriate reporting of suspected fraud and corruption, including but not limited to the requirements of MP 0125/19 *Notifiable and Reportable Conduct Policy* • providing advice and support to the Chief Executive/Director General, Executive Committee and line managers relating to fraud and corruption issues • remaining up-to-date with current best practice • reviewing and evaluating the FCC System at least every two years.

Role	Accountabilities
Information and Communications Technology (ICT)	Health Support Services (HSS) provides ICT services to maintain and support the safe and reliable functioning of computer technology and information systems. HSS ICT are responsible for: • maintaining cybersecurity standards, policies and risk management activities • providing security and cybersecurity (of non-physical/internet connected computer systems) of information systems to ensure integrity of the entire network • monitoring and reporting of internal threats, and external controls of cyber and security threats from external parties • supporting identification and coordination of cybersecurity events, incidents and investigations • developing and implementing cyber security training.
Records Management	Records management is responsible for developing and implementing policies and plans which ensure the security of corporate information in accordance with the *State Records Act 2000*. Records management facilitate Records Awareness Training for all staff.
Internal Audit Unit	The Internal Audit Unit is responsible for: • evaluating the risk of fraud and corruption found through internal audit activities • providing objective assurance as to the effectiveness of controls in mitigating, detecting and reporting fraud events • reporting any suspected fraud and corruption found during scheduled activities of Internal Audit.
External Audit	External audit carry out audit procedures which include aiming to detect material misstatements in the entity’s financial statements due to fraud. The governing body and/or Audit and Risk Committee undertake discussions with the auditor in terms of the audit procedures that will be carried out and take a proactive position in relation to the audit fraud detection program including: • informing the auditor of the entity’s fraud and corruption detection philosophy and the importance the entity places on fraud detection as part of the audit • aiding the auditor to enable a more comprehensive examination of fraud and corruption issues • an internal consideration of fraud risk factors as defined in The Auditor’s Responsibilities Relating to Fraud in an Audit of a Financial Report Issued by the Auditing and Assurance Standards Board (ASA 240).

Role	Accountabilities
Risk Unit	The Risk Unit is responsible for: • developing and maintaining the risk management framework, including as it relates to fraud and corruption risks • providing advice and support to the relevant Audit and Risk Committee, Chief Executive/Director General, Executive Committee and line managers relating to fraud and corruption risk management • maintaining the risk register and reporting on risk management performance.
Human Resources	Human Resources receive reports of suspected fraud or corruption from staff and take appropriate steps to address the concerns reported including referring the matter to the Integrity Unit.
Public Interest Disclosure (PID) Officers	PID officers are responsible for investigating information disclosed, or causing that information to be investigated, and taking action following the completion of the investigation in accordance with the relevant provisions of the *Public Interest Disclosure Act 2003* (PID Act).

2.2 Fraud and corruption risk management

Risk management is integral to an entity's risk culture and an essential component of effective internal control. As such, it should be integrated into all entity activities and functions[1].

Treasurer's Instruction 825 – Risk Management (TI825) requires entities to develop and periodically assess risk management policies and practices. Where possible, entity risk management policies and processes should be consistent with the Risk Management Guidelines (AS ISO 31000:2018) which provide guidance on effective and efficient risk management and can be used to manage any type of risk. Aligning risk management policy, frameworks and supporting documentation to AS ISO 31000:2018 is a requirement of HSPs pursuant to MP 0006/16 *Risk Management Policy*. The Department of Health *Risk Management Policy* prescribes the Department of Health has adopted MP 0006/16 *Risk Management Policy*. Where MP 0006/16 refers to a HSP, this also refers to the Department of Health.

Fraud and corruption are business risks which require assessment and treatment in the same way as other risks. The policy requires entities to ensure risks of fraud and corruption are regularly assessed, and identified risks are addressed and managed appropriately. The FCC System must:

- document the entity's fraud and corruption risk controls as they relate to staff, volunteers, students on placement and business associates
- document the entity's controls for the:

1. **Prevention of fraud and corruption**
2. **Detection of fraud and corruption**
3. **Response to allegations or the identification of fraud and corruption.**

Fraud and corruption risk assessments establish the level, nature, form and likelihood of fraud and corruption related risk exposures. Like any risk assessment process, assessments of fraud and corruption related risks must be conducted as an ongoing, iterative process. This will maximise the opportunity to identify and treat all fraud and corruption related risks. Consideration

[1] *Treasurer's Instruction 825 - Risk Management*

of risk factors includes both internal and external environments and addresses all business processes.

Core business areas, for which fraud and corruption risks are important considerations include:

- information and communications technology, including cybersecurity
- information management, including access, use and disclosure of information
- finance, including revenue collection and use of purchasing cards
- procurement and contract management
- recruitment and appointment
- payroll services, including salaries, leave, benefits and allowances
- capital works, infrastructure and maintenance
- outsourced functions and funded service delivery programs.

2.3 Implementing an Information Security Management System

Entities depend on effective information security management to protect the confidentiality, integrity and availability of health information and systems. MP 0067/17 *Information Security Policy* outlines the security controls required to be implemented, monitored and reviewed by entities.

MP 0067/17 *Information Security Policy* aligns to the principles of the Australian Standards but does not require entities to implement the Information Security Management System (ISMS) which is a minimum requirement of AS 8001:2021.

2.4 Record keeping and confidentiality of information

Poor record-keeping is a fraud and corruption risk. Failure to keep accurate, complete and secure records hinders fraud and corruption prevention, detection and response, including:

- undisclosed or poorly managed conflicts of interest
- inappropriate acceptance of gifts, hospitality, donations or similar benefit
- inadequate risk assessment and control
- increased exposure to technology-enabled fraud
- increased risk of the release of confidential information
- loss of corporate information
- lack of procedural integrity
- inaccurate or invalid data analytics
- ineffective internal audit
- lack of evidence of wrongdoing to support disciplinary or criminal matters
- inability to evaluate internal controls
- non-compliance with policy and legislation.

Compliance with mandatory WA health system policies, as summarised in Table 2, meets the AS 8001:2021 minimum requirements:

- policies, procedures and systems that require staff to maintain accurate and complete records of business activity exist
- policies, procedures and systems:

  - set out mechanisms for identifying and protecting information that is confidential
  - establish criteria for monitoring compliance and taking any necessary corrective action
  - regard any deliberate failure to maintain complete and accurate records as a disciplinary matter.

Table 2: Mandatory WA health system policies related to record keeping and confidentiality of information

Policy	Policy Requirements
MP 0124/19 *Code of Conduct Policy*	Maintaining records in accordance with expected standards is required of all staff in accordance with the Code of Conduct. Any deliberate failure to maintain complete and accurate records is a breach of the Code of Conduct which may result in disciplinary action.
MP 0015/16 *Information Access, Use and Disclosure Policy* and the Department of Health *Information Access, Use and Disclosure Policy*	MP 0015/16 *Information Access, Use and Disclosure Policy* requires HSPs to: • understand when information is authorised to be accessed, used or disclosed • access, use, disclose and share information in a manner that protects the privacy of patients including sensitive, confidential and appropriately classified information • protect information from misuse and inappropriate access and disclosure • establish internal controls and/or audits to ensure policy compliance • take all reasonable steps, to ensure information is protected from misuse, interference, loss, unauthorised access or modification. • ensure local policies, tools, processes, awareness training and education programs enable staff to: ○ secure and protect sensitive, confidential and appropriately classified information ○ do everything reasonable and practicable to prevent the misuse or unauthorised access to or disclosure of information. The Department of Health *Information Access, Use and Disclosure Policy* places similar requirements on Department of Health employees.
MP 0135/20 *Information Breach Policy*	Ensures that misuse and inappropriate access, use, disclosure and/or loss of information held within entities is investigated and solutions are identified and implemented to mitigate future breaches. Requires employees to immediately notify the relevant Integrity Unit when an information breach has occurred. Requires line managers and/or the entity delegated authorities to: • determine if misconduct may have contributed to the information breach

Policy	Policy Requirements
	- report any potential misconduct as per MP 0124/19 *Code of Conduct Policy*.
MP 0152/21 *Information Management Governance Policy*	Outlines the minimum Information Management Governance standards for entities.
MP 0144/20 *Information Retention and Disposal Policy*	Requires entities to maintain appropriate local plans, policies and/or procedures to ensure compliance with State Records Commission endorsed Retention and Disposal Schedules.

3. Fraud and corruption prevention

The Department CEO, as the System Manager, is committed to ensuring robust governance structures and processes are in place to prevent all forms of fraud and corruption. Entities rely on a variety of strategies to minimise the opportunity for fraud and corruption. The following strategies are considered effective aspects of the FCC System:

- promoting a sound integrity framework
- raising awareness of fraud and corruption
- managing conflicts of interest
- managing risks connected to gifts, hospitality, donations and similar benefits
- implementing and maintaining an internal control system
- workforce screening
- screening and ongoing management of business associates.

3.1 Promoting a sound integrity framework

Effectively communicating and promoting the FCC System internally within the entity and, where appropriate, externally to the entity assists in promoting a culture of integrity.

Compliance with mandatory WA health system policies, as summarised in Table 3, meets some of the AS 8001:2021 minimum requirements:

- an integrity framework is developed
- the integrity framework includes a Code of Ethics or Code of Conduct incorporating high-level aspirational statement of values with examples of conduct the entity deems unacceptable
- the implementation of the integrity framework (including prevention of fraud and corruption) is done through the application of risk management practices and risk-based approach (outlined in AS ISO 31000:2018).

Entities can leverage these policies to meet the remaining AS 8001:2021 minimum requirements by:

- using a participatory approach to developing integrity governance arrangements to build commitment within the entity
- communicating and promoting the integrity framework and the FCC System internally within the entity and, where appropriate, externally to the entity
- including a process for benchmarking and for continuous monitoring of the entity's integrity environment, which may include compliance monitoring with integrity policies and reporting
- ensuring observable adherence to the entity's integrity governance arrangements by the governing body and executive
- incorporating a statement of commitment by the governing body to establish and maintain an integrity environment and to actively promote such a culture
- allocating and/or delegating responsibilities for the integrity governance structure, processes and systems such as adequate dedicated resources/staffing to ensure the entity's integrity governance arrangements and initiatives are implemented and monitored
- clearly communicating internally that every person associated with the entity has a role to play in driving positive integrity and ethical behaviours

- establishing a relevant committee for overseeing the operation and maintenance of the entity's integrity governance arrangements and integrity related matters
- incorporating an integrity standard into performance management/development.

Table 3: Mandatory WA health system policies related to promoting a sound integrity framework

Policy	Policy Requirements
MP 0124/19 *Code of Conduct Policy*	Identifies the CORE values fundamental to the WA health system and translates these values into principles that guide conduct in the workplace.
MP 0114/19 *Integrity Governance Policy*	Requires documented integrity governance arrangements which incorporate integrity promotion, mandatory training and education for all staff, including AEDM training as mandated by Commissioner's Instruction No. 40 Ethical foundations. Requires integrity governance arrangements to be consistent with the entity's established risk management practices and aligned to MP 0006/16 *Risk Management Policy* (which requires policy, frameworks and other supporting documentation to be aligned with AS ISO 31000). Note: the Department of Health *Risk Management Policy* prescribes the Department of Health has adopted MP 0006/16 *Risk Management Policy*. Where MP 0006/16 refers to a HSP, this also refers to the Department of Health.

3.2 Raising awareness of fraud and corruption

It is the responsibility of all executives to promote a culture of integrity and to encourage staff to identify and speak out against fraudulent and corrupt acts within their entity. Statements made regularly and consistently by entities which clearly articulate a zero tolerance for fraudulent or corrupt practices are important for promoting awareness and communicating the expected integrity standards to staff. Promoting the support mechanisms available and that staff must not attempt to intimidate, coerce, take reprisal or retaliate against those who disclose can encourage staff to report suspected fraud and corruption. Fraud and corruption awareness training increases the likelihood that fraud and corruption will be detected through reporting mechanisms[2].

The policy prescribes entities must undertake actions to ensure all staff understand their role in the prevention and detection of fraud and corruption and how to respond if they detect or suspect fraud or corruption.

MP 0114/19 *Integrity Governance Policy* requires integrity governance arrangements to incorporate integrity promotion, mandatory training and education for all staff. Integrity promotion and education may include information regarding:

- the roles and accountabilities of staff for fraud and corruption control
- fraud and corruption related risks
- indicators fraudulent and corrupt activity
- information regarding how staff can report fraud and corruption

[2] Occupational Fraud 2022: A Report to the Nations; Association of Certified Fraud Examiners.

- periodic reinforcement of fraud and corruption controls.

To meet the requirements of AS 8001:2021, the awareness raising program must be delivered regularly, appropriate to the entity's exposure to fraud and corruption risk and so that it is relevant and useful to the position and role of each person in the entity.

In addition to mandatory AEDM training, awareness strategies may include information delivered via:

- intranet articles
- email alerts
- print media
- leadership driven information sessions
- targeted training to high risk groups/services.

An effective integrity promotion strategy supports awareness and communication with consumers, business associates and other third parties regarding options to report concerns in relation to possible corrupt conduct by staff, volunteers, students on placement and business associates.

3.3 Managing conflicts of interest

Failure to declare conflicts of interest creates a risk that may undermine the public's trust and confidence in the WA health system and may present opportunities for fraud or corruption.

Compliance with mandatory WA health system policies, as summarised in Table 4, meets some of the AS 8001:2021 minimum requirements:

- a policy and/or procedure that requires staff to disclose actual, potential or perceived conflicts of interest exists
- records of relevant business, financial, family, political or personal interests of staff that could conflict with their entity-wide duties are maintained
- records of actions taken to avoid, eliminate or manage any perceived, potential and/or actual conflicts of interest identified are maintained
- information about conflicts of interest is included in relevant training programs
- a failure to disclose or properly manage a conflict of interest is treated as a potential disciplinary matter.

Entities can leverage these policies to meet the remaining AS 8001:2021 minimum requirements by:

- binding relevant business associates to MP 0138/20 *Managing Conflicts of Interest Policy*, including treating a failure to disclose or properly manage a conflict of interest as a potential breach of contract
- requiring management to monitor and actively manage risks posed by conflicts of interest
- ensuring all staff complete AEDM training, which includes information about conflicts of interest, including secondary employment as covered by Section 102 of the PSMA
- promoting these policies in other relevant training programs
- seeking to identify concealed conflicts of interest as part of the entity's fraud and corruption detection program.

Table 4: Mandatory WA health system policies related to conflicts of interest

Policy	Policy Requirements
MP 0124/19 *Code of Conduct Policy*	Requires that staff must: 2.4. Avoid situations which may give rise to pecuniary or other conflicts of interest and immediately declare any conflicts of interest, or possible perceptions of such conflicts of interest, to their manager. 2.5. Disclose any personal or professional matters that may lead to actual or perceived conflicts of interest. 2.6. Ensure their actions and decisions are not influenced by self-interest, considerations of personal gain or other improper motives. 2.7. Not accept inducements or incentives that are intended to influence their decisions or actions. 2.10. Familiarise themselves and act in accordance with MP 0138/20 *Managing Conflict of Interest Policy*, MP 0136/20 *Gifts Benefits and Hospitality Policy*, and section 102 of the PSMA.
MP0114/19 *Integrity Governance Policy*	Requires documented integrity governance arrangements which incorporate integrity promotion, mandatory training and education for all staff, including AEDM training as mandated by Commissioner's Instruction No. 40 Ethical foundations.
MP 0138/20 *Managing Conflicts of Interest Policy*	Ensures a consistent approach to integrity governance and risks associated with conflicts of interest across the WA health system, and ensures effective governance of conflicts of interest including monitoring, evaluation and reporting. Includes key definitions of conflicts of interest. Requires recording of all declared conflicts of interest, the authorised person's decision and management plan using the System Manager Conflicts of Interest Declaration Registry (**COIR**).
MP 0047/17 *Sponsorship Policy*	Sets out the process and documentation requirements when seeking to enter into a sponsorship agreement.

Further guidance about managing the risks associated with conflicts of interest is provided in the Integrity Coordinating Group's Conflicts of interest – Guidelines for the WA public sector.

3.4 Managing risks connected to gifts, hospitality, donations and similar benefits

Accepting gifts, hospitality, donations and similar benefits creates a risk that may undermine the public's trust and confidence in the WA health system and may present opportunities with the potential to escalate into bribery or corruption.

Compliance with mandatory WA health system policies, as summarised in Table 5, meets some of the AS 8001:2021 minimum requirements:

- a policy on gifts, hospitality, donations and similar benefits is documented
- records of gifts, hospitality, donations and similar benefits are maintained
- information about managing gifts, hospitality, donations and similar benefits is included in relevant training programs.

Table 5: Mandatory WA health system policies related to gifts, hospitality, donations and similar benefits

Policy	Policy Requirements
MP 0124/19 *Code of Conduct Policy*	Requires that staff must: 2.8. Not accept gifts which are, or could reasonably be interpreted to be, designed to secure influence or preferential treatment in favour of the giver. 2.9. Disclose any gift or benefit received or intended to be accepted in accordance with the MP 0136/20 *Gifts Benefits and Hospitality Policy*. 2.10. Familiarise themselves and act in accordance with the MP 0138/20 *Managing Conflict of Interest Policy*, MP 0136/20 *Gifts Benefits and Hospitality Policy*, and section 102 of the PSMA.
MP 0136/20 *Gifts, Benefits and Hospitality Policy*	Ensures a consistent approach to the integrity governance and risks associated with gifts, benefits and hospitality offered to staff members, and ensures the effective governance of offered gifts, benefits and hospitality. Includes key definitions of gifts, benefits and hospitality. Requires recording of all gifts, benefits and hospitality offered and the authorised person's decision using the System Manager Gift Declaration Registry (GDR) database.
MP 0114/19 *Integrity Governance Policy*	Requires documented integrity governance arrangements which incorporate integrity promotion, mandatory training and education for all staff, including AEDM training as mandated by Commissioner's Instruction No. 40 Ethical foundations.
MP 0047/17 *Sponsorship Policy*	Sets out the process and documentation requirements when seeking to enter into a sponsorship agreement.
WA Health Financial Management Manual - 530 Receiving Donations	Prescribes how donations of money, goods, assets and services are to be managed.
WA Health Staff Air Travel Policy	Includes requirements related to sponsored travel.

Entities can leverage these policies to meet the remaining AS 8001:2021 minimum requirements by:

- monitoring gifts, hospitality, donations and similar benefits by analysing the records which these policies require to be maintained
- maintaining records of actions taken relation to breaches of these policies in the System Manager Case Management System (CMS)
- ensuring all staff complete AEDM training, which includes information about managing gifts, hospitality, donations and similar benefits
- promoting these policies in other relevant training programs
- reviewing compliance with these policies annually.

Further guidance about managing the risks of gifts, benefits and hospitality is provided in the Public Sector Commission (PSC) Good practice guidance for WA public authorities.

3.5 Implementing and maintaining an internal control system

Proactive anti-fraud and anti-corruption controls play a key role in an entity's fight against fraud and corruption. The presence of these controls is associated with smaller losses and quicker detection[3]. While the presence of these mechanisms alone does not ensure all fraud and corruption will be prevented, commitment to and investment in targeted prevention and detection measures send a clear message to consumers, staff, volunteers, students on placement, business associates and others about the entity's anti-fraud and corruption stance.

It is important all business processes, particularly those assessed as having higher predisposition to the risks of fraud and corruption, are subject to a rigorous system of internal controls which are documented, accessible, reviewed and updated regularly and understood by all staff. The following are considered effective anti-fraud and anti-corruption controls:

- compliance with Policy Frameworks which specify the requirements that all entities must comply with in order to ensure effective and consistent activity across the WA health system
- formal fraud and corruption risk assessment
- code of conduct
- implementing an ISMS
- management review of controls, processes etc for adherence to local policies and expectations
- internal and external audit
- fraud and corruption awareness training
- accessible and anonymous fraud and corruption reporting mechanisms
- proactive data analytics
- position rotation, leave management and ensuring positions are backfilled during periods of leave
- physical security.

The operating effectiveness of internal controls must be regularly assessed, and weak or failed internal controls remediated.

3.6 Workforce screening

A thorough workforce pre-engagement screening process, including for employees, volunteers and students of placement, is considered to be an effective way of reducing the potential exposure to internal fraud and corruption by obtaining a higher level of assurance as to the integrity, identity and credentials of people employed by an entity[4].

Entity recruitment processes and pre-engagement screening must be undertaken in accordance with MP 0033/16 *Recruitment Selection and Appointment Policy*, MP 0136/19 *Pre-Employment Integrity Check Policy*, *Criminal Record Screening Policy and Guidelines* and MP 0176/22 *Working with Children Check Policy*, as well as any other screening relevant to the role.

[3] Occupational Fraud 2022: A Report to the Nations; Association of Certified Fraud Examiners.
[4] Australian Standard AS 8001:2021 Fraud and corruption control

To meet the AS 8001:2021 minimum requirements, screening must be conducted in accordance with *Employment Screening* (AS 4811-2006) which exceeds the requirements of WA health system policy.

Some strategies entities can consider include:

- ensuring recruitment practices verify work history information provided by applicants and include referee checking
- verifying the applicant’s declared qualifications and professional memberships
- re-screening staff upon promotion or change of employment circumstances particularly if the person is being promoted to a senior position or a position involving higher risk of fraud or corruption
- re-screening staff prior to the completion of the probation period.

3.7 Screening and ongoing management of business associates

The WA health system has a duty to engage with reputable business associates and comply with relevant legislation as it relates to procurement practices. Rigorous screening processes give confidence and assurance entities should be working with a particular business associate[5].

Ensuring staff engaging with business associates take steps to ensure the bona fides of new business associates and periodically confirm the bona fides of continuing business associates, is an important fraud and corruption prevention strategy. The due diligence required may vary depending on the assessed fraud and corruption risk in relation to specific transactions, projects, activities involving the particular business associate.

Checking the bona fides of a business associate may include:

- searching open source locations such as the internet and social media for any adverse reports on the business associate, their key controllers such as the owner/s, the CEO and/or senior manager/s
- consulting with other public departments or private companies who engage with the business associate to identify any concerns
- confirming the business associate has the required licences or educational qualifications
- evaluating any suspicious activity observed during the life of the relationship, such as presentation of incomplete, incorrect or inflated invoices.

AS 8001:2021 prescribes detailed minimum requirements for the screening of business associates.

[5] Strengthening integrity in financial management; Public Sector Commission.

4. Detecting fraud and corruption

Improving how an entity detects fraud and corruption can increase staff's perception fraud will be detected and might help deter future incidents[6]. The following strategies are considered effective aspects of the FCC System:

- vigilance and awareness of all staff, encouraged and supported through the entity's promotion of a sound integrity framework and fraud and corruption awareness training and education
- systems for reporting suspected fraud and corruption
- identifying early warning signs
- data analytics, including the analysis of financial records
- exit interviews[7]
- internal and external audit activities
- internal control systems
- operational risk management processes.

4.1 Reporting suspected fraud and corruption

Research consistently shows the most common method for detecting fraud and corruption is from reports by staff and other interested parties[8]. An effective and trusted reporting system is the best way to identify fraud and corruption early and expose weak internal control systems.

The policy prescribes the FCC System must include mechanisms to enable internal and external parties to report suspected fraud and corruption and include processes for meeting external reporting requirements.

Compliance with mandatory WA health system policies, as summarised in Table 6, meets some of the AS 8001:2021 minimum requirements:

- a program for detection of fraud and corruption events, which establishes a range of fraud and corruption reporting channels for staff, is implemented
- adequate means for reporting suspicious or known illegal or unethical conduct are available to all staff.

Entities can leverage these policies to meet the remaining AS 8001:2021 minimum requirements by:

- including a range of channels for reporting fraud and corruption, as well as suspicious or known illegal or unethical conduct, as part of the entity's program for detection of fraud and corruption events
- encouraging staff, volunteers, students on placement, business associates and third parties who have concerns or suspicions of fraudulent or corrupt conduct to come forward and promptly report them, through the entity's awareness raising program
- establishing a system for handling complaints in line with *Guidelines for Complaint Management in Organisations* (AS/NZS 10002)[9]

[6] Occupational Fraud 2022: A Report to the Nations; Association of Certified Fraud Examiners.
[7] AS 8001:2021 requires entities adopt a program of exit interviews for all terminated staff.
[8] Occupational Fraud 2022: A Report to the Nations; Association of Certified Fraud Examiners.
[9] For HSPs, adherence to MP 0130/20 *Complaints Management Policy* may meet this requirement.

- training frontline and communications staff in recognising and escalating complaints about fraud and corruption
- allowing anonymous reporting.

Table 6: Mandatory WA health system policies related to reporting improper conduct

Policy	Policy Requirements
MP 0124/19 *Code of Conduct Policy*	As part of demonstrating commitment to the Code of Conduct, all staff must take responsibility to identify and report conduct that is not consistent with the Code of Conduct. Any staff member that has reason to believe that a breach of the Code of Conduct has occurred should refer the matter to their manager in the first instance. If the staff member is not comfortable reporting a suspected breach to their manager, they should report the matter to a more senior officer.
MP 0127/20 *Discipline Policy* and the Department of Health *Discipline Policy*	Requires that for all complaints or incidents which may concern a breach of discipline, entities must ensure: • a consistent process for the assessment and management of suspected breaches is applied • documented arrangements exist for the processes related to the: ○ receipt of complaints, or any information received regarding a staff member's/employee's conduct ○ assessment of the information conducted for the purposes of meeting notifying obligations pursuant to CCM Act.

4.1.1 Public Interest Disclosures

One of the reasons a person may not report suspected fraud or corruption is a fear of reprisal. The PID Act allows people to make disclosures, including anonymous disclosures, about wrongdoing and protects them when they do.

AS 8001:2021 provides detailed minimum requirements for entities to consider when implementing a PID management system.

4.2 Identification of early warning signs

Ineffective oversight, especially when coupled with weaknesses in other internal systems and controls, presents a real risk of inappropriate behaviour. Entities must be alert to early warning signs which may be indicators of fraud and corruption. The Occupational Fraud 2022: A Report to the Nations found 85% of perpetrators demonstrated at least one behavioural red flag while committing fraud or corruption. This may include staff who:

- avoid taking leave, excess leave must be managed in accordance with MP 0100/18 *Management of Accrued Leave Policy* for HSPs, the Leave Management Procedure for the Department of Health, and relevant WA health system industrial instruments
- work excessive hours
- live a lifestyle above apparent means
- experience financial difficulties, or other difficulties in their personal life
- react poorly when questioned to avoid further scrutiny
- delay or avoid audits and reviews without good reason

- are overly controlling, avoid sharing duties, refuse to train other staff or do not delegate responsibilities
- destroy or do not keep records to support decisions
- have overly familiar relationships with suppliers
- habitually cut corners on policy and process requirements
- have previous conduct, work performance or legal issues.

AS 8001:2021 requires entities to implement a program for detection of fraud and corruption events by identification of early warning signs that is appropriate for the entity's assessed fraud and corruption exposures.

4.3 Data analytics

Entities have access to various sources of data which may be used to assist in the detection of fraud and corruption, including:

- CMS
- GDR
- COIR
- Travel system
- Leave and timesheet records
- Procurement Development and Management System
- Records management system
- Financial management systems.[10]

Designing and applying data analytic tests that capture relevant indicators of the entity's fraud or corruption exposures is necessary to meet the requirements of AS 8001:2021.

[10] AS 8001:2021 requires post-transactional review and analysis of management accounting reports to detect fraud and corruption

5. Responding to fraud and corruption events

Effective response planning allows entities to react to a suspected fraud or corruption event in a measured and consistent manner to protect the entity from financial, reputational, industrial and legal risks.[11] All actions taken, and evidence captured, in response to a fraud and corruption event must be documented to ensure the adequacy of the internal control environment can be assessed to prevent similar events in the future.

AS 8001:2021 requires entities to incorporate a programmed response to fraud and corruption events in a response and recovery plan which clearly sets out the entity's response to detected fraud and corruption events. The response and recovery plan forms part of the FCC System.

The following are considered effective aspects of the response and recovery plan:

- immediate actions in response to a fraud and corruption event, including fraud or corruption by a business associate
- crisis management and business continuity, especially if senior staff are implicated
- managing the impact of fraud or corruption on consumers, staff, volunteers, students on placement, business associates and third parties
- capture of evidence, including digital evidence[12]
- internal and external reporting
- investigation and disciplinary processes
- recovery of funds or property, including through insurance
- assessment and enhancement of internal controls.

5.1 External reporting

The policy prescribes the FCC System must include processes for meeting external reporting requirements. The CCM Act places obligations on entities to notify the PSC of suspected minor misconduct and the Corruption and Crime Commission (**CCC**) of suspected fraud, corruption or serious misconduct.

Fraud and corruption may also constitute notifiable conduct under the *Health Practitioner Regulation National Law (WA) Act 2010* (**National Law**). The National Law requires that if an entity reasonably believes a staff member who is a registered health practitioner has behaved in a way that constitutes notifiable conduct, the entity must notify the Australian Health Practitioner Regulation Agency of the notifiable conduct.

Section 146(1) of the HS Act reiterates this requirement, and also requires HSPs to notify the Department CEO. Section 146(2) of the HS Act requires HSPs to notify the Department CEO on becoming aware that a staff member has been charged, convicted or found guilty of fraud or corruption.

For HSPs, compliance with mandatory WA health system policies, as summarised in Table 7, meets most of the AS 8001:2021 minimum requirements:

- a policy on whether and how allegations of fraudulent and corrupt conduct are reported to the police, other appropriate law enforcement agency, or other government body exists

[11] Fraud Response Management: Is your organisation prepared to execute an efficient and effective response?; Deloitte. 2009.
[12] Refer to *Information Technology – Security Techniques – Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence* ISO/IEC 27037.

- relevant obligations form part of the external reporting policy
- the external reporting policy is consistently applied so that there can be no suggestion of selective application.

Table 7: Mandatory WA health system policies related to external reporting of fraud and corruption

Policy	Policy Requirements
MP 0124/19 *Code of Conduct Policy*	Requires HSPs to assess whether a suspected breach of the Code of Conduct is Notifiable or Reportable Conduct and notify the CCC and/or the PSC, the Western Australian Police, and/or the Department CEO.
MP 0127/20 *Discipline Policy*	Requires documented arrangements exist for the processes related to the: • assessment of the information conducted for the purpose of meeting notifying obligations pursuant to the CCM Act and MP 0125/19 *Notifiable and Reportable Conduct Policy*.
Department of Health *Discipline Policy*	Requires documented arrangements exist for the processes related to the: • assessment and referral of complaints and information for the purposes of meeting notification and reporting obligations for suspected minor and serious misconduct pursuant to s.4 CCM Act.
MP 0125/19 *Notifiable and Reportable Conduct Policy*	Requires HSPs to ensure that: • Reportable and Notifiable Conduct (that requires reporting to the Department CEO in accordance with sections 146 and 167 of the HS Act), is: ○ reported using the Reporting Conduct Template. • Suspected criminal offences are reported to the Police.

HSPs can leverage these policies to meet the remaining AS 8001:2021 minimum requirements by:

- in the event that a decision is made to refer the matter to the appropriate law enforcement agency, giving an undertaking to the law enforcement agency that the HSP will do all that is reasonable in assisting the agency to conduct a full and proper investigation.[13]

For the Department of Health, the Integrity Governance Framework includes the process through which the Department of Health notifies the CCC of serious misconduct, the PSC of minor misconduct and WA Police of criminal behaviour. The Department of Health *Information Access, Use and Disclosure Policy* supports a culture of information sharing that promotes the access, use and disclosure of information when it is permitted or required by law. Compliance and consistent application of the these meets the AS 8001:2021 minimum requirements.

[13] Section 220 of the *Health Services Act 2016* provides for the authorised disclosure of information.

5.2 Investigation of suspected fraud or corruption

Investigation of a suspected fraud or corruption event provides insight into the effectiveness of internal controls. Where a suspected fraud or corruption event has been reported externally, for example to the CCC, the external body may investigate.

If the investigation is to be managed by the entity, it is vital the investigation is conducted by appropriately skilled and experienced staff who are independent of the business unit in which the alleged fraudulent or corrupt conduct occurred. Entities may also choose to engage an external investigator.

MP 0127/20 *Discipline Policy* and the Department of Health *Discipline Policy* require entities to ensure documented arrangements exist for the processes related to investigations. AS 8001:2021 contains detailed requirements regarding investigations including:

- principles for conducting investigations
- investigation planning
- skills, qualification, training and safety of investigators
- capture, analysis and management of evidence
- record keeping and confidentiality.

5.3 Disciplinary procedures

Fraud or corruption by an employee is a breach of discipline as defined in section 161 of the HS Act and section 80 of the PSMA.

Compliance with mandatory WA health system policy, as summarised in Table 8, meets the AS 8001:2021 minimum requirements:

- the Human Resources Manual (or other relevant internal policies or guidelines) includes particulars on how disciplinary proceedings should be conducted
- a process exists for ensuring the findings of an investigation into a fraud or corruption event are referred by the investigation function to an independent person or committee (the decision maker).

Table 8: Mandatory WA health system policy related to disciplinary procedures

Policy	Policy Requirements
MP 0127/20 *Discipline Policy* and the Department of Health *Discipline Policy*	For all complaints or incidents which may concern a breach of discipline, requires entities to ensure: • a consistent process for the assessment and management of suspected breaches of discipline is applied • appropriately skilled officers assess and manage the matters • documented arrangements exist for the processes related to the: ○ receipt of complaints, or any information received regarding a staff member's/employee's conduct ○ investigations ○ appointment of the decision maker and any change to the decision maker ○ recording of all decisions made and that decisions are transparent and capable of review, including the rationale

	for the decision that reflects their assessment of the seriousness of the matter ○ management of case records. • procedural fairness is applied.

5.4 Internal reporting and escalation

Regular and robust internal reporting of fraud and corruption events is required to enable the governing body to ensure the entity has in place adequate anti-fraud and anti-corruption measures.

Compliance with mandatory WA health system policies, as summarised in Table 9, meets some of the AS 8001:2021 minimum requirements:

- a system for the capturing all detected fraud and corruption events is developed and implemented
- a fraud and corruption event register is established and all fraud and corruption events occurring (subject to minimum reporting thresholds) are entered therein[14]
- the fraud and corruption event register is maintained by the entity's specialist fraud and corruption control resource (where appointed) or other responsible person
- a program for the centralised capture of all fraud and corruption events is implemented.

Entities can leverage these policies to meet the remaining AS 8001:2021 minimum requirements by:

- implementing a system for the reporting, analysis and escalation of all detected fraud and corruption events
- ensuring that data captured in the CMS is used in the effective measurement of fraud and corruption against or by the entity.

Table 9: Mandatory WA health system policies related to internal reporting of fraud and corruption events

Policy	Policy Requirements
MP 0124/19 *Code of Conduct Policy*	Requires entities to monitor compliance with MP 0124/19 *Code of Conduct Policy*.
MP 0127/20 *Discipline Policy* and the Department of Health *Discipline Policy*	Requires for all complaints or incidents which may concern a breach of discipline, entities to ensure: • all matters are recorded in the CMS, as soon as reasonably practicable, in accordance with the CMS Protocols.

5.5 Recovery of stolen funds or property

Remedies are available to entities for loss to the State by staff members, including through overpayment recovery processes. The *WA Health* *Financial Management Manual*, specifically section 244, provides information about the recovery of official losses.

In addition, where criminal proceedings commence and the penalty for any offence committed is more than two years of imprisonment, the State may take action under the *Criminal Property Confiscation Act 2000* to recover properties and monies owed to the State. Whether the likely

[14] Entities may choose to maintain a separate fraud and corruption event register in addition to the CMS.

benefits of such recovery will exceed the funds and resources invested in the recovery action is an important consideration for entities.

To meet the requirements of AS 8001:2021 entities must have a policy requiring consideration of legal action for recovery of stolen funds or property where there is evidence of fraud or corruption and where the benefits of such recovery are considered worthwhile.

5.6 Insuring against fraud events

Pursuant to *Treasurer's Instruction 812 – Insurance* (**TI812**), entities must ensure an appropriate level of insurance cover over all insurable risks, including fraud and corruption risks. Compliance with TI812 meets the requirements of AS 8001:2021.

Insurance is available with the Western Australian Government Treasury Managed Fund (RiskCover), managed and administered by the Insurance Commission of Western Australia, including:

- liability cover for claims made against the entity resulting from unlawful, fraudulent, dishonest, criminal or malicious acts of employees
- property and business interruption cover for loss of property insured resulting from fraudulent or dishonest acts (including computer fraud) by employees or other persons
- cyber cover for liability arising from data protection risk exposures, the management of personal data and the consequences of losing corporate information.

The WA Health Financial Management Manual, specifically sections 242 and 244, provides information about insurance including initiating insurance claims.

5.7 Assessing internal controls, system and processes post detection of a fraud or corruption event

In each instance where fraud or corruption is detected, the reassessment of the adequacy of the internal control environment, particularly those controls which directly impact the event, and consideration whether improvements are required, is critical.

Compliance with mandatory WA health system policy, as summarised in Table 10, meets some of the AS 8001:2021 minimum requirements:

- in each instance where a fraud or corruption event is detected the adequacy of the internal control environment is reassessed (as part of risk review and continuous monitoring of the risk profile).

Table 10: Mandatory WA health system policy related to risk governance

Policy	Policy Requirements
MP 0006/16 *Risk Management Policy*	Requires HSP Boards to ensure that: • a local risk management policy, framework and any other supporting documentation, aligned with *Risk Management – Guidelines* AS ISO 31000:2018, is developed and includes: ○ defined processes to identify, assess, treat, monitor, review, record and report risks ○ risk review frequency requirements ○ oversight requirements for the governing body and/or dedicated risk and audit sub-committee (or equivalent)

	• risk identification and continuous monitoring of the risk profile occurs on an ongoing basis. Note: the Department of Health *Risk Management Policy* prescribes the Department of Health has adopted MP 0006/16 *Risk Management Policy*. Where MP 0006/16 refers to a HSP, this also refers to the Department of Health.

Entities can leverage this policy to meet the remaining AS 8001:2021 minimum requirements by:

- conveying relevant findings from an investigation report to the process and risk owners to allow risks to be re-evaluated and treated
- ensuring the internal control review process assesses the adequacy of the internal control environment, considers whether improvements are required and makes recommendations aimed at improved mitigation of fraud and corruption risks
- including the concept of "disruption"[15] as part of the suite of initiatives to improve the mitigation of fraud and corruption risks
- reporting all remedial action proposed in response to a fraud or corruption event to the relevant Audit and Risk Committee which shall be responsible for ensuring that all remedial action in relation to internal controls has been affected
- where remediation or enhancements are required, implementing these as soon as practicable
- allocating responsibility for monitoring internal control remediation following an investigation into a fraud or corruption event to an individual with significant authority
- periodically analysing the body of investigation reported in order to identify relevant trends, patterns or areas for internal control improvement.

[15] AS 8001:2021 includes initiatives that can be used to disrupt fraud or corruption.

Glossary

Term Used	Definition
Accountable and Ethical Decision Making (AEDM) training	A training program to support staff to make accountable and ethical decisions.
AS 8001:2021	Fraud and corruption control Australian Standard.
Bona fides	Evidence showing that a person or organisation's business practices are straightforward and of integrity.
Bribe	A gift or benefit offered or solicited by a staff member to influence that person to act in a particular way and to induce the staff member to act in a way that is contrary to the known rules of honesty and integrity.
Business Associate	External party with whom an entity has, or plans to establish, some form of business relationship. A business associate includes, but is not limited to: • contractors • consultants • public private partnerships • recruitment agencies • students on placement • sub-contractors • suppliers • universities and TAFE colleges • volunteers.
Case Management System (CMS)	The database administered by the System Manager provided to entities to enter, track and report cases of conduct that may concern a breach of discipline.
Conflict of interest	A situation arising from conflict between the performance of public duty and private or personal interests. Conflicts of interest may be actual, or be perceived to exist, or potentially exist at some time in the future.
Conflicts of Interest Registry (COIR)	An electronic database to record all conflicts of interest. It records the date the declaration was made and by whom, the nature of the conflict, the type of conflict (actual, potential or perceived) and proposed management plan. It details the authorised person's decision in relation to the conflict, documents the agreed management plan and the approval of the management plan.
Corruption	Corruption is defined by Australian Standard AS 8001:2021 as: "*Dishonest activity in which a person associated with an organisation (e.g. 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 advantage or advantage for another person or organisation*".

Term Used	Definition
	Corruption is any conduct that is improper, immoral or fraudulent and may, under certain circumstances include but is not limited to: • serious conflict of interest • dishonestly using influence • manipulation of procurement process • acceptance of gifts and hospitality • acceptance of a bribe • misuse of information systems, internet or email • unauthorised release of confidential, private information or intellectual property. Corruption is a serious offence as prescribed by s. 80A of the *Public Sector Management Act 1994*.
Department CEO	The Chief Executive Officer (Director General) of the Department of Health.
Fraud	Fraud is defined by Australian Standard AS 8001:2021 as "*dishonest activity causing actual or potential gain or loss to any person or organisation including theft of moneys or other property by persons internal and/or external to the organisation and/or where deception is used at the time, immediately before or immediately following the activity*". Fraud can take many forms, examples of situations which, in certain circumstances, may include fraud are: • theft or obtaining property, financial advantage or any other benefit by deception • unauthorised use of credit / purchasing card • false timesheets, sick or annual leave claims • providing false or misleading information, or failing to provide information where there is an obligation to do so • causing a loss, or avoiding or creating a liability by deception • making, using or possessing forged or falsified documents • unlawful use of computer systems, vehicles, telephones and other property or services • manipulating expenses or salaries. Fraud is a serious offence as prescribed by s. 80A of the *Public Sector Management Act 1994*.
Fraud and Corruption Control System	A framework for controlling the risks of fraud and corruption against or by an organisation.

Term Used	Definition
Gift Declaration Registry (GDR)	An electronic database to record all declarable gifts benefits and hospitality. It records the date an offer was made and by whom, the nature of the offer, its estimated value, the raising of any actual, potential or perceived conflicts of interest or reputational risks and how the offer was managed. For accepted offers, it details the business reason for acceptance and the officer approving the acceptance.
Information Security Management System	A set of interrelated and interacting elements that establishes, implements, operates, monitors, reviews, maintains and improves information security.
Integrity	The expected standards of behaviour and actions of Department of Health employees or HSP staff members which reflect honesty, accountability, transparency, impartiality, and acting with care and diligence.
Integrity governance	The formal arrangements by which an organisation establishes, monitors and evaluates structures, systems and processes to promote a culture of integrity, and appropriately respond to issues. Integrity governance structures include mechanisms to escalate risks, to the peak governance body of the organisation, for review and action.
Interested parties	A person or organisation that can affect, be affected by, or perceive itself to be affected by a decision or activity.
Investigation	A systematic process to discover the facts/particulars relating to the complaint/incident that may concern a breach of discipline and leads to the examination and analysis of the evidence. All investigations must result in or lead to an outcome.
Minor Misconduct	Pursuant to section 3 and 4(d) of the *Corruption Crime and Misconduct Act 2004*, Minor Misconduct is conduct by a Public Officer that: (i) adversely affects, or could adversely affect, directly or indirectly, the honest or impartial performance of the functions of a public authority or public officer, whether or not the public officer was acting in their public officer capacity at the time of engaging in the conduct or (ii) constitutes or involves the performance of functions in a manner that is not honest or impartial or (iii) involves a breach of the trust placed in the public officer by reason of their office or employment as a public officer or (iv) involves the misuse of information or material that the public officer has acquired in connection with their functions as a public officer, whether the misuse is for the benefit of the public officer or the benefit or detriment of another person and

Term Used	Definition
	(v) constitutes, or could constitute, a disciplinary offence providing reasonable grounds for termination of a person's office or employment.
Notifiable and reportable conduct	Conduct by a staff member that: • is suspected on reasonable grounds to constitute or may constitute professional misconduct or unsatisfactory professional performance as defined in accordance with section 5 of the *Health Practitioner Regulation National Law (WA) Act 2010* (reportable to the Department CEO pursuant to section 146(1) of the *Health Services Act 2016* • relates to a charge for a Serious Offence (reportable to the Department CEO pursuant to section 146(2) of the *Health Services Act 2016* • may concern a suspected breach of discipline under sections 160, 161 and 162 of the *Health Services Act 2016* • concerns suspected Minor Misconduct or Serious Misconduct as defined in accordance with section 4 of the *Corruption Crime and Misconduct Act 2004* (notifiable to the Corruption and Crime Commission or the Public Sector Commission pursuant to section 28 or 45D of the *Corruption Crime and Misconduct Act 2004*).
Position rotation	Rotating staff in positions with a high risk of fraud and corruption within an entity, or temporary rotation to perform a short term project or a similar role on a short term basis in another entity or public agency.
Public Interest Disclosure (PID)	An appropriate disclosure of public interest information to a proper authority.
Serious Misconduct	Pursuant to section 3 and 4(a) (b) and (c) of the *Corruption Crime and Misconduct Act 2004*, Serious Misconduct is conduct by a Public Officer who – (a) acts corruptly or corruptly fails to act in the course of their duties or (b) corruptly takes advantage of their office or employment to obtain a benefit or to cause a detriment to any person or (c) acting in the course of their duties or while deliberately creating the appearance of acting in the course of their duties, commits an offence punishable by two or more years imprisonment. Corrupt conduct tends to show a deliberate intent for an improper purpose or an improper motivation. Corrupt conduct may involve an exercise of a public power or function but for private benefit. It may involve conduct such as the deliberate failure to perform the functions of office properly, or the exercise of a power or duty for an improper purpose.)
Serious offence	Has the same meaning as section 80A of the *Public Sector Management Act 1994.*

Term Used	Definition
	Serious Offence means: (a) an indictable offence against a law of the State (whether or not the offence is or may be dealt with summarily), another State or a Territory of the Commonwealth or the Commonwealth (b) an offence against the law of another State or a Territory of the Commonwealth that would be an indictable offence against a law of this State if committed in this State (whether or not the offence could be dealt with summarily if committed in this jurisdiction) (c) an offence against the law of a foreign country that would be an indictable offence against a law of the Commonwealth or this State if committed in this State (whether or not the offence could be dealt with summarily if committed in this jurisdiction) (d) an offence, or an offence of a class, prescribed under section 108 (see Offences Prescribed).
Technology-enabled fraud	Fraud against or by an entity which relies heavily on information technologies and which would not be possible without information technologies.
WA health entities	WA health entities include: (i) health service providers as established by an order made under section 32 (1)(b) of the *Health Services Act 2016*. (ii) Department of Health as an administrative division of the State of Western Australia pursuant to section 35 of the *Public Sector Management Act 1994*.

This document can be made available in alternative formats on request for a person with disability.