Fraud and corruption control policy

1 Purpose

This policy identifies the minimum requirements and the responsibilities for the prevention, detection and response in relation to suspected fraud and corruption within the Department of Communities, Housing and Digital Economy (the department).

This policy applies to all persons working for and with the department. This includes employees working for the department (regardless of whether they are permanent, fixed-term temporary, full-time, part-time or casual employees and/or on secondment from another department) and other persons who perform work for the department including contractors, students gaining work experience and volunteers. For the purposes of this policy, the term contractor includes on-hired temporary labour services (agency staff).

The policy:

- ensures that all persons working for and with the department act legally, ethically and in the public interest
- enables all persons working for and with the department to understand their responsibilities to prevent fraud and corruption occurring in the department, and
- should be read in conjunction with the Integrity Framework and the other relevant policies listed in Attachment 3.

2 Policy statement

Fraud and corruption have the potential to cause significant financial, reputational and service delivery harm to the department. These forms of wrongdoing also have a potential to diminish or damage community confidence in the department.

Accordingly, the department has no tolerance towards fraud and corruption. This is supported by a hierarchy of governance and controls which contributes to and support our ethical culture.

The department recognises that fraud and corruption prevention and control are integral components of good governance and risk management.

The department is committed to effectively preventing, detecting and responding to incidents or threats of fraud and corruption, both internal and external, including through:

PREVENTION	• actively fostering a **robust integrity framework** to maintain a strong ethical culture • implementing effective **departmental wide anti-fraud and anti-corruption policies** • **management commitment** to preventing, detecting and responding to fraud and corruption • undertaking **employment screening** on persons proposed to be engaged by the department, which may include, but is not limited to, checking criminal history, blue card, referees and serious discipline history • **training** in the requirements of the Code of Conduct for the Queensland Public Service (Code of Conduct) • implementing **other education and awareness initiatives** aimed at maintaining continued high standards of professional and ethical conduct • implementing, sustaining and monitoring **effective preventative controls** (for example, separation of duties and access controls) • **publicly communicating** the department's commitment to the highest standards of professional conduct and honest and ethical business practices

DETECTION	• undertaking regular reviews to assess **fraud and corruption risks** contained in operational risk registers • implementing appropriate **internal controls** which address the department's operating environment and specific risks • encouraging and supporting the **internal and external reporting** of suspected wrongdoing • **strategically using information systems** to detect suspected fraud
RESPONSE	• **effectively assessing and dealing with suspected wrongdoing** through the Integrity Services Unit • **supporting persons** who make Public Interest Disclosures (PIDs) • **external reporting** to regulatory entities, such as the Crime and Corruption Commission (CCC), the Queensland Police Service and the Queensland Audit Office pursuant to legislative requirements • **taking appropriate action** in respect to substantiated fraud and corruption, which may include: – undertaking a disciplinary process, which may result in disciplinary action, including termination of employment – referring matters to the Queensland Police Service – de-registering suppliers so they are unable to perform work for the department – pursuing the recovery of losses – implementing action to prevent reoccurrence

3 Responsibilities

Key roles and responsibilities are as follows:

3.1 Director-General

The Director-General is responsible for:

- ensuring that the department has appropriate policies, training and awareness initiatives and other control systems to prevent, detect and effectively manage fraud and corruption
- ensuring impartiality and integrity in the performance of the department's functions
- ensuring accountability and transparency in the department's operational performance
- visibly promoting and communicating, both within the department and externally, that high standards of professional conduct and honest and ethical business practices are expected
- encouraging and supporting the reporting of suspected wrongdoing
- ensuring appropriate action is taken with respect to proven allegations of fraud and corruption.

3.2 Board of Management

The Board of Management (BoM) is responsible for:

- ensuring the effective management of risk through:
  - setting the organisation's risk culture and appetite and monitoring key departmental risks
  - ensuring fraud and corruption risk assessment occurs at departmental and business area levels
- periodically reviewing complaint information (including complaints of fraud and corruption)
- taking appropriate action to prevent fraud and corruption.

3.3 Divisional Heads and departmental managers

Divisional Heads, business area heads and other departmental managers are responsible for:

- displaying ethical leadership and high standards of behaviour consistent with the Code of Conduct
- ensuring all persons working for and within their division/work area:
  - are made aware of their fraud and corruption control responsibilities, including the requirement to report suspected wrongdoing
  - comply with relevant policies and procedures, and
  - where applicable, complete the required mandatory training/induction about public sector ethics, including the Code of Conduct
- ensuring that appropriate and effective internal controls are in place in their division/work area
- effectively managing risk in accordance with the department's Risk Management Framework
- promoting and supporting whole-of-department fraud and corruption prevention initiatives
- taking prompt and appropriate action to prevent fraud and corruption, including pro-actively managing staff conduct
- advising the Integrity Services Unit of all suspected fraud and corruption
- ensuring appropriate and timely action is taken regarding proven allegations of fraud and corruption
- ensuring that recommendations arising from audits and investigations are treated as a priority and actioned promptly.

3.4 Deputy Director-General, Strategy and Corporate Services

In addition to the responsibilities set out in 3.3, the Deputy Director-General, Strategy and Corporate Services is responsible for ensuring that fraud and corruption risk management is integrated into the department's operational risk management processes.

3.5 Integrity Services Unit

The Integrity Services Unit is responsible for:

- developing and maintaining integrity-related policies and procedures
- promoting an ethical culture and appropriate decision making through fraud and corruption prevention initiatives
- reporting complaints of fraud and corruption on a periodic basis to the BoM
- reporting on all fraud and corruption matters in accordance with relevant legislation
- managing and independently investigating complaints involving fraud and corruption, which may constitute suspected corrupt conduct and/or a PID in accordance with departmental policy and legislative requirements
- providing independent advice regarding fraud and corruption matters to the Director-General, Divisional Heads, the Chief Finance Officer, the Chief Human Resources Officer and other departmental managers.

3.6 Internal Audit Unit

The Internal Audit Unit is responsible for:

- assessing the adequacy and effectiveness of internal controls within business areas as part of routine auditing activities
- making recommendations to improve the effectiveness of key controls where required

- developing and executing selected data analytics programs to detect fraud and corruption
- providing advice to business areas in relation to preventing and detecting fraud and corruption.

3.7 Finance

In accordance with the *Financial Accountability Act 2009*, Finance (through the Chief Finance Officer) is responsible, for:

- establishing, maintaining and reviewing financial internal controls
- providing the Director-General with an annual assurance statement on the efficiency and effectiveness of the financial internal controls.

3.8 Governance, Planning and Reporting

The Governance, Planning and Reporting team is responsible for:

- overseeing the department's risk management system, policy and framework
- coordinating risk reporting to Divisional Heads and the BoM
- facilitating risk management capability and maturity, including coordinating the divisional Risk Management Coordinators network
- maintaining risk management guidance documents, training resources and other tools and templates.

3.9 Information technology

Technology and Digital Solutions (through the Chief Information Officer) is responsible for:

- establishing, maintaining and reviewing technology-based prevention controls
- establishing, maintaining and reviewing information and communications technology (ICT).

The Digital Business Group is responsible for:

- establishing, maintaining and reviewing information management policy and supporting documents
- facilitating ongoing enhancements of an Information Security Management System that is aligned with Information Standard 27001.

3.10 Human Resources

Human Resources is responsible for:

- coordinating, through the Chief Human Resources Officer, the effective implementation of department-wide education and training initiatives about public sector ethics, including the Code of Conduct
- providing advice on all relevant employment legislation (for example, the *Public Service Act 2008*), industrial instruments (for example, certified agreements and awards) and directives (for example, recruitment and selection)
- providing advice on appropriate management action and/or disciplinary proceedings regarding alleged fraud and corruption by an employee of the department
- liaising with the relevant external authorities to manage pre-employment screening activities.

3.11 All persons working for and with the department

All persons working for and with the department are responsible for:

- acting in an ethical manner in the workplace
- understanding and complying with all policies and procedures including:
  - safeguarding assets, information and other resources under their control
  - ensuring all administration is accurate with no deliberate omissions (for example, claiming allowances appropriately, recording accurate hours of work on timesheets and properly applying for leave)
  - registering gifts and benefits offered, accepted and/or given in accordance with the relevant policy
  - declaring all perceived, potential and actual conflicts of interest
  - immediately reporting all wrongdoing including suspicions of fraud and corruption – IN CONFIDENCE – to:
    - the Director-General or
    - the Deputy Director-General, Strategy and Corporate Services or
    - the Chief Human Resources Officer or
    - the Integrity Services Unit or
    - a departmental supervisor/manager or
    - the Crime and Corruption Commission
- where applicable, completing mandated training/induction about public sector ethics, including the Code of Conduct.

Every person working for or with the department is responsible for taking appropriate action to prevent fraud and corruption and report suspected fraud and corruption of which they become aware.

4 Delegations

N/A

5 Reporting requirements

The Integrity Services Unit are responsible for reporting instances of fraud and corruption to external agencies (such as the Crime and Corruption Commission and the Queensland Police Service) pursuant to legislative requirements.

6 Human rights

The policy has been reviewed for compatibility with human rights under the *Human Rights Act 2019* (the Act). The policy has been found to limit human rights only to the extent that is lawful, reasonable, and demonstrably justifiable in accordance with section 13 of the Act therefore, it is reasonable to conclude that the policy is compatible with human rights.

7 Approval

This policy was approved by the Director-General on 18 August 2022.

Attachment 1: Contacts

Attachment 2: References

Attachment 3: Definitions

Attachment 4: Areas of perceived high fraud and corruption risk in the public sector

Attachment 5: Examples of types of fraud and corruption that may be relevant to the department

Attachment 6: Identifying fraud and corruption risks

Attachment 7: Indicators of fraud and corruption (‘red flags’)

Licence

Version Control

Version	Date	Comments
1	18 August 2022	Policy approved

Attachment 1: Contacts

Director-General
Department of Communities, Housing and Digital Economy
1 William Street
Brisbane Qld 4000
GPO Box 2457
Brisbane Qld 4001
Telephone (07) 3017 5801

Deputy Director-General, Strategy and Corporate Services
Department of Communities, Housing and Digital Economy
Level 23, 111 George Street
Brisbane Qld 4001
Telephone (07) 3097 8515

Chief Human Resources Officer
Department of Communities, Housing and Digital Economy
Level 16, 111 George Street
Brisbane Qld 4001
GPO Box 2457
Brisbane Qld 4001
Telephone (07) 3008 3039

Director, Integrity Services Unit (CCC Liaison officer and PID Coordinator)
Department of Communities, Housing and Digital Economy
Telephone (07) 3109 4897
Email: integrityservices@chde.qld.gov.au

Crime and Corruption Commission
Complaints Section
Level 2, North Tower Green Square
515 St Pauls Terrace
Fortitude Valley Qld 4006
GPO Box 3123
Brisbane Qld 4001
Telephone (07) 3360 6060
Facsimile (07) 3360 6333
Toll Free 1800 061 611 – outside Brisbane, within Queensland
www.ccc.qld.gov.au

Attachment 2: References

The requirements set out in this document are based on, and are consistent with, relevant Government legislation, regulations, directives, information standards and/or policies at the time of publication.

Examples are:

Legislation and regulations

Criminal Code Act 1899 (Sections: 408C, 441, 442, 442B, 442BA)

Crime and Corruption Act 2001

Financial Accountability Act 2009

Financial and Performance Management Standard 2019

Public Interest Disclosure Act 2010

Public Sector Ethics Act 1994

Public Service Act 2008

Queensland Government documents

Code of Conduct for the Queensland Public Service

Corruption in focus: A guide to dealing with corrupt conduct in the Queensland public sector, Crime and Corruption Commission, January 2020

Financial Accountability Handbook

Legal protections for Queensland Government employees, indemnity guideline

Department of Communities, Housing and Digital Economy documents

Attendance recording policy

Complaints Management Policy

Complaints Management Procedure

Conflicts of interest policy

Corporate card purchasing policy

Corrupt conduct prevention policy

Criminal history screening policy

Data governance policy

Delegations

Discipline policy

Financial management practice manual

Fraud and corruption control plan

Gifts and benefits policy

Hospitality policy

Information security management policy

Insurance policy

Integrity Framework

Intellectual property policy

Public interest disclosure policy

Risk Management Policy

Risk Management Framework

Sponsorship policy

Standard of conduct policy for contractors, subcontractors, consultants, students and volunteers

Taxi services policy

Travel policy

Use of ICT services, facilities and devices policy

Vehicle policy

Workplace behaviour policy

Other Resources

Australian Standard 8001—2021 Fraud and Corruption Control[1]

[1] The Australian Standard 8001 2021 Fraud and Corruption Control is not a mandatory standard, however it was considered in the development of this policy as best practice.

Attachment 3: Definitions

Term	Description
Corrupt conduct	As per s 15(1) of the *Crime and Corruption Act 2001*, means conduct of a person (regardless of whether the person holds or held an appointment) that: • adversely affects, or could adversely affect (directly or indirectly) the performance of functions or the exercise of powers of a unit of public administration or a person holding an appointment; and • results, or could result, directly or indirectly, in the performance of functions or the exercise of powers mentioned above in a way that— ▪ is not honest or is not impartial; or ▪ involves a breach of the trust placed in a person holding an appointment (either knowingly or recklessly); or ▪ involves a misuse of information (or material) acquired in or in connection with the performance of functions or the exercise of powers of a person holding an appointment; and • would, if proved, be a criminal offence; or a disciplinary breach providing reasonable grounds for terminating the person's services (if the person is or were the holder of an appointment). As per s 15(2) of the *Crime and Corruption Act 2001*, corrupt conduct also means conduct of a person (regardless of whether the person holds or held an appointment) that: • impairs, or could impair, public confidence in public administration; and • involves, or could involve, any of the following – ▪ collusive tendering ▪ fraud relating to an application for a licence, permit or other authority under an Act with a purpose or object of any of the following (however described)— o protecting health and safety of persons o protecting the environment o protecting or managing the use of the State's natural, cultural, mining or energy resources; ▪ dishonestly obtaining, or helping someone to dishonestly obtain, a benefit from the payment or application of public funds or the disposition of State assets ▪ evading a State tax, levy, duty or otherwise fraudulently causing a loss of State revenue ▪ fraudulently obtaining or retaining an appointment; and • would, if proved, be a criminal offence; or a disciplinary breach providing reasonable grounds for terminating the person's services (if the person is or were the holder of an appointment). Corrupt conduct can be attributed to any person, regardless of whether or not they are employed in the department, including: • employees • people who used to but no longer work in the department • people who subsequently take up an appointment in the department • people who are suppliers or providers to the department • other private individuals or organisations

Term	Description
	• people outside Queensland where there is a direct link between the conduct and its adverse effect on the department).[2] Refer to the Corrupt conduct prevention policy for further information.
Corruption	Means a 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 advantage or advantage for another person or organisation. This definition is based on the Australian Standard Fraud and Corruption Control (AS 8001-2021).
Divisional Heads	Means the Queensland Government Chief Customer and Digital Officer, all Deputy Directors-General and Associate Director-General.
Fraud	Means a 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. Property in this context also includes intellectual property and other intangibles such as information. 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. While conduct must be dishonest for it to meet the definition of 'fraud', the conduct need not necessarily represent a breach of the criminal law. This definition is based on the Australian Standard Fraud and Corruption Control (AS 8001-2021).

[2] "Corruption in focus: A guide to dealing with corrupt conduct in the Queensland public sector", Crime and Corruption Commission, January 2020, page 1.3.

Attachment 4: Areas of perceived high fraud and corruption risk in the public sector

The following table outlines key functional areas in government agencies that the Queensland Audit Office has identified as being the most prone to fraud.[3]

Agency function, program or activity	Potential fraud risks
Procurement	• Fraudulent procurement by an employee or contractor • Fraudulent procurement practices by vendors • Fraudulent influence by an employee on panel arrangements or preferred supplier lists • Fraudulent contract management by an employee • Deliberately over-ordering resources to use the surplus for personal gain
Finance	• Fraudulent use of a corporate card • Fraudulent invoices requesting payment to false bank details • Misappropriation of cash • Misuse of CabCharge for personal use or profit • Seeking to award a grant outside the terms of the agreement and conditions for personal benefit • Claims for reimbursement for non-work related expenses
Human resources	• Nepotism in recruitment and selection processes • Corruption in promotion processes • Bias against an applicant in recruitment and selection processes • Deliberate manipulation of recruitment selection panels • Fraudulent deception by an applicant in recruitment and selection processes • Management knowingly concealing the corrupt conduct of subordinate employees
Payroll	• Fraudulent recording of overtime, allowances, penalties, or leave taken • Fraudulent manipulation of the rostering process • Inappropriate changes to master files • Fraudulent claims for study assistance
Assets	• Misappropriation of materials for private use or sale • Misappropriation of motor vehicles for private use or sale • Manipulation of a public auction or public tender process for disposal of assets
Reporting	• Fraudulent operational reporting by management • Fraudulent reporting to meet KPIs • Fraudulent reporting to meet government -imposed FTE limits • Manipulation of financial results (for example, non-accrual of expenses at year end to improve performance or over accrual to spend budget) • Manipulation of financial results to spend the allocated budget
Information	• Fraudulent disclosure of confidential information by an active or terminated employee for personal gain • Fraudulent disclosure of politically sensitive information • Destruction of public records to enable a cover-up

[3] This information has been derived from the Queensland Audit Office's Fraud risk assessment and planning tool.

Attachment 5: Examples of types of fraud and corruption that may be relevant to the department

The following are provided as examples only and are not exhaustive. Any resemblance to actual conduct is purely coincidental.

Human Resources

- A job applicant uses false credentials or documents (for example, a false work history or qualifications) to obtain employment.
- A job applicant deliberately fails to disclose relevant criminal history during a recruitment and selection process.
- A member of a selection panel does not disclose a personal or professional relationship with an applicant to favour the applicant.
- Timesheets are falsified to claim time or payments.
- Medical certificates are falsified to obtain paid time off work.
- Job statements or official documentation are falsified to conceal absence from duty.
- An employee makes false phone calls to generate call outs and overtime.
- False claims are made (for example, workers' compensation claims or allowance claims).
- "Phantom" employees are placed on the payroll with salaries diverted to an employee's own bank account.
- Employees deliberately fail to report overpayments.
- Former employees continue to receive departmental payments and do not disclose this.
- An employee impersonates a supervisor or manager.
- An employee directs a contractor to perform work at their private residence and to invoice the department.

Procurement

- Documents are falsified to obtain approval for payment.
- Signatures are forged on payment approval documentation.
- False invoices from fake or actual suppliers are submitted for payment.
- A panel member does not disclose a relationship with an offeror, so as to favour the offeror.
- Kickbacks or other rewards/benefits are provided to an employee on a procurement panel for a favourable assessment.
- Bid rigging (for example, prior to submitting bids, suppliers arrange who will win the tender and at what price).
- Price fixing (for example, suppliers agree on a pricing structure for goods and services).

Assets (including technology and information)

- Using others' passwords in payment systems and making payments to a personal bank account.
- An employee or agency staff takes an asset home falsely claiming it is not working and needs to be disposed of.
- A property is purchased at a higher than market value in exchange for a kickback.
- Falsification of departmental vehicle logs to conceal private use.
- Accessing government databases/systems to view personal information of the community (including clients) and/or government employees for non-work purposes.

Finance

- Stealing funds by diverting funds to a fake account which appears to be a genuine payee.
- A false payment instruction is created, with forged signatures.
- Some cash is taken before (cash) receivables are recorded.
- Improper revenue recognition (for example, recording false sales, over/under estimating percentage of work completed on long-term contracts).
- Orders are split to avoid delegation limits.

- False statements are made (for example, to conceal losses, inflate the value of receivables, provide false stock counts).
- Travel is undertaken for predominantly personal purposes but recorded as official travel.
- Deliberately underestimating the value of a gift.

Other

- A supervisor falsely reports that work by a contractor has been completed to a satisfactory standard, in return for a kickback or other reward/benefit from the contractor.
- Rewards/benefits are provided to an employee on a funding/grants panel for favourable outcome of funding/grants application.

Attachment 6: Identifying fraud and corruption risks

The Queensland Audit Office has listed factors to consider when identifying potential fraud risks.

Category	Attribute	Factors that increase fraud risk	Fraud exposure
Financial	Materiality of economic flows	High value/low volume, and/or high volume/low value transactions with third parties.	Fraud risk increases in both likelihood and consequence as the sums involved increase.
	Nature of transactions	Non-exchange/non-reciprocal where values given do not match values received, e.g. grants, subsidies, donations, rates and other involuntary transfers.	Unlike a commercial exchange, the inability to readily compare or reconcile the value of what was provided with the value of what was received increases the opportunity for fraud and the likelihood that it remains undetected.
	Susceptibility to manipulation	Accounting balances require subjective measurements involving high levels of judgement or expertise to calculate.	The manipulation of accounting balances can be used to conceal frauds or may itself be fraudulent by concealing losses or adverse financial positions.
Relationships	Economic dependency	High supplier dependency—supplier relies on the entity for a significant proportion of its gross turnover/continued solvency.	Supplier dependency creates an incentive for the supplier to offer bribes and an opportunity for the purchaser to request kick-backs to retain business.
		High remuneration dependency—salary at risk or other performance incentive schemes with large bonuses or earn-outs arrangements relative to base salary contingent upon achieving targets.	Overly aggressive or unrealistic performance targets can motivate employees to commit fraud to conceal or overstate actual performance or can be used to rationalise fraud when bonuses are not paid.
	Market depth	Limited market depth restricting competition, existence of oligopoly or monopoly suppliers.	Lack of competition creates opportunities for collusive tendering, and for predatory pricing or other cartel behaviours.
	Proximity to external parties	High degree of direct, face-to-face contact required. Interaction with customers and suppliers at their premises or in the field.	Ongoing personal contact away from direct supervision establishes the opportunity to cultivate inappropriate personal relationships or to groom others to unknowingly facilitate frauds.

Category	Attribute	Factors that increase fraud risk	Fraud exposure
	Related parties	Related party transactions—employees or their spouse, children, and other close relatives or associates have a direct or indirect personal pecuniary interest in transactions or confidential information.	Personal interests inherently conflict with public interest and motivate fraudulent behaviour.
		Non-commercial, non-arm's length transactions.	Transaction values that are not set by reference to observable market inputs create the opportunity for fraud.
Attitudes	Internal controls	Failure to quickly address or remediate internal control issues identified by auditors and other parties.	Failure by management to demonstrate a commitment to strong and effective control fosters weak control consciousness and a poor control culture that increases the opportunity both for fraud to occur and for it to remain undetected.
		Corner-cutting, failure to follow due process is tolerated or encouraged.	
		Senior leadership does not promote good governance.	
	Transparency/ accountability	Reluctance to voluntarily disclose information publicly.	Failure to acknowledge mistakes, to accept blame and to report risks fosters a culture of secrecy which increases the risk that unusual or suspect transactions and behaviours will not be reported.
		Limited or poor quality internal reporting to executive.	
Use of assets	Intrinsic value of physical assets	Use of highly 'portable and attractive' items of equipment.	Movable equipment and machinery and items of cash or negotiable instruments are inherently more susceptible to theft or misappropriation by employees.
		Handling of cash or other assets readily convertible into cash.	
	Intrinsic value of intangibles	Access to commercially sensitive/economically valuable information not publicly available, e.g. intellectual property.	The intangible nature of sensitive information makes it difficult to secure and to prevent being misused for personal gain or advantage.
Decision making	Assignment of authority	Decision making is widely devolved to business units.	The further removed the approval and scrutiny of transactions are from the 'centre' and from the 'top' of the organisation the greater potential for fraud to remain undetected.
		Authority is highly delegated below senior management.	

Category	Attribute	Factors that increase fraud risk	Fraud exposure
	Decentralisation of operations	Operations in locations remote from central office.	The 'tyranny of distance' makes it harder to establish consistent processes and to understand how controls are being applied.
		Span of management.	
	Discretion	Personal discretion applied in determining allocations to third parties.	Staff or elected officials with the discretion to determine how funds are allocated to third parties have the ability to over-ride standard processes and expose their organisation to fraud.
	Supervision	Span of control is high.	Lack of supervision creates the opportunity for staff to commit fraud and that it remains undetected e.g. paying for goods and services that were never received.

Attachment 7: Indicators of fraud and corruption ('red flags')

Awareness of warning signs (red flags) for possible fraud or corruption is a useful method of detection. The more interrelated the indicators identified, the higher the risk of potential fraud or corruption.

For further information or to report suspected fraud or corruption, contact the department's Integrity Services Unit by email integrityservices@chde.qld.gov.au.

Behavioural Red flags

Persons who:

- consistently work longer hours than their colleagues, where there is no apparent reason
- infrequently take time off for holidays, or not at all
- attempt to hide their work or are very secretive about the work they're doing
- are known to be under personal financial pressure
- suddenly have a significant lifestyle change
- are aggressive or defensive when challenged, and/or controlling of certain colleagues
- are subject to consistent complaints
- are consistently breaking the rules
- are reluctant to provide information, delay providing information or provide different information (for example, explanations) to different people
- request that internal audits are delayed so they have adequate time to "prepare"
- request a significant level of information about proposed internal audit scopes
- predominantly use the one supplier
- don't adhere to procurement procedures.

Financial Red flags

- Cash only transactions
- Higher than normal costs which are not readily explainable
- A large volume of refunds
- Unusually large inventories
- Unusual transactions (even if only for small amounts)
- Persons who make a higher than normal number of mistakes, especially where these lead to a loss
- Persons with unexplained sources of wealth
- Persons who have competing personal business interests
- Persons who submit inconsistent and/or unreasonable expense claims.

Procedural Red flags

- Persons who make procedural or system enquiries which are not related to their duties
- Prospective employees who provide incomplete, inaccurate or inconsistent information as part of employment applications
- Persons who excessively micro-manage
- Insufficient oversight/audit applied
- Suppliers who insist on dealing with just one employee
- Supplier invoices which look different to previous invoices issued by the same supplier
- Attempts to obtain sensitive information such as usernames, passwords and credit card details (for example, phishing emails, whaling attacks)
- Anomalies associated with requests to change supplier bank account details (for example, a request received from an email account not associated with the supplier)
- Lack of transparency
- Too much delegation without proper review procedures.