Fraud and Corruption Control Policy

Purpose

To set out Diabetes Australia's principles for controlling fraud and corruption, including conflicts of interest and acceptance of gifts and hospitality, entertainment and sponsored travel.

As a 'for purpose' organisation, DA's reputation for integrity and appropriate management of funds, donations and bequests is critical in maintaining confidence in our ability to manage programs and services for people living with diabetes and those at risk. Strong fraud and corruption control processes enables us to maximise benefits to those we support.

Scope

This document applies to all the Workforce, this includes:

- The DA Board
- All employees of DA, whether permanent, casual, full-time, part-time, or trainees
- Volunteers and work experience placements
- Entities or persons providing goods and services to DA (including contractors and subcontractors).

This policy has been drafted in consideration of DA's operating environment, size and associated fraud and corruption risks. The requirements, policies and/or best practice principles set out in the *Additional References section* have informed the development of this policy and should be read in conjunction with this policy where appropriate.

Guiding Principles

Integrity

All the Workforce are expected to act with the utmost integrity. DA promotes a culture of integrity and ensures that all employees at all levels are aware of their responsibilities for maintaining integrity through awareness training.

Fraud and Corruption Control

DA has no appetite for fraudulent or corrupt conduct and is committed to ensuring robust governance and ethical conduct of all of the Workforce fulfilling functions on our behalf.

We are committed to preventing fraud and corruption through:

- procedures for reporting conflicts of interest, gifts, benefits and hospitality
- preventative controls such as workplace screening, physical security, and controls for preventing technology-enabled fraud
- strong financial controls
- training and awareness programs
- design of incentives, performance indicators

- initiative design and development that includes consideration of fraud and corruption
- setting expectations with our contractors and subcontractors
- detective controls such as internal audit, data analytics, complaints monitoring and whistleblower processes

All identified or suspected instances of fraud will be promptly investigated, with all available legal remedies explored. This includes termination of employment, reporting to internal and external oversight committees and bodies, referral of the matter to law enforcement for potential criminal prosecution and civil recovery of financial losses.

Responsibilities

All Workforce

- Have a basic understanding of fraud and corruption and related behaviours.
- Declare actual, potential or perceived conflicts of interest in writing and self-report any changes in circumstances as you become aware of them.
- Declare gifts, benefits and hospitality.
- Comply with the Commonwealth Supplier Code of Conduct.
- Report suspicions or incidences of fraud and corruption.
- Speak up, through Whistleblowing or other channels, when something this isn't right.
- Co-operate with activities to prevent, detect and respond to fraud and corruption, including investigations.
- Participate in awareness and training sessions.

Board of Directors

- Approves the Fraud and Corruption Control Policy and strategies.
- Ensures adequate resources are allocated for fraud and corruption control initiatives.
- Monitors and reviews the effectiveness of the Fraud and Corruption Control Framework.
- Ensures reasonable steps are taken as set out in Governance Standard 5 of the ACNC, relating to behavioural duties.
- The Board may delegate duties relating to fraud and corruption control management to the Risk Quality and Compliance (RQC) Committee in accordance with their Terms of Reference.

Group Chief Executive Officer (GCEO)

- Ensures enforcement of the organisation's Fraud and Corruption Control Policy.
- Promotes a culture of integrity and ethical behaviour.
- Applying the Public Interest Disclosure Act 2013 (PID Act) and the appointment of Authorised Officers.
- Overseeing compliance with National Anti-Corruption Commission Act 2022 and mandatory reporting requirements.
- Actioning signification findings in relation to fraud or corruption.

Authorised Officers / Principal Officer

Authorised Officers are appointed by the GCEO, including but not limited to the Chief Governance Legal and Risk Officer.

Chief of Governance Legal and Risk (CGLR)

- Central point to consistently manage all disclosures.
- Act as an Authorised Officer to receive and investigate whistleblowing disclosures under the PID Act, and assess compliance with other relevant acts as relevant to the subject matter of the disclosure.
- Oversees implementation of whistleblower policy.
- Coordinates fraud and corruption incident response actions, including legal considerations.

Chief Risk Officer (CRO)

- Provides expertise on fraud and corruption control.
- Identifies and assesses fraud and corruption risks across DA, including oversight of risk assessments and maintenance of a risk register.
- Development and oversight of fraud and corruption awareness training and communication program.
- Oversees periodic review of fraud and corruption controls, either as part of targeted fraud risk assessments or separately.

Qualified Investigator

- Investigate suspected fraud or corruption incidents and report findings to Management and the RQC Committee.
- May be internal or external depending on the determining factors of each case.
- Must not have any potential or perceived conflicts of interest in relation to the case.

Chief of Corporate Services and Chief Financial Officer (CCS and CFO)

- Ensures appropriate financial controls are in place to detect and prevent fraud.
- Oversees financial reporting and compliance with relevant standards and regulations.
- Reviews allegations of financial fraud and takes necessary corrective actions.
- Ownership for prevention of technology-enabled fraud and corruption including engagement of external monitoring service to provide a range of brand protection, including domain monitoring, fake ads, fraudulent listings, and executive impersonation.

Executive Leadership Team, Group Executive and Managers

- Visibly promote and communicate high standards of professional conduct and honest and ethical practices.
- Encourage the reporting of fraud, corruption, and misconduct.
- Ensure appropriate action is taken in respect of proven incidents of fraud, corruption, and misconduct.
- Ensure that whistleblowers are supported and protected in accordance with our policy.
- Review and manage risk mitigation plans for direct reports, as relevant to conflicts of interest, and accepting gifts hospitality entertainment and sponsored travel.
- Identify and assist with implementing controls to manage declared conflicts of interest
- Review and monitor the effectiveness of controls, relevant to fraud and corruption control, the values and codes of conduct (internal and supplier).
- Escalate any issues or concerns relating to declared conflicts of interest to the CGLR or CRO.
- Identify and escalate any breaches of DA's values and codes of conduct (internal and supplier) to the Chief People Officer who may escalate potential PIDs to the CGLR.

Internal Audit Team

- Monitors and reports on the effectiveness of fraud and corruption risk management strategies.
- Conducts regular audits to assess the effectiveness (both design and operating) of internal controls in preventing and detecting fraud and corruption, risks and controls.
- Conducts data analysis to identify any fraud and corruption red flags.

Chief Information Officer (CIO)

- Implements robust cybersecurity measures to protect against fraud and corruption.
- Ensures strict controls are in place for access of systems including those which hold personal or sensitive information.
- Regularly monitors IT systems for signs of suspicious activity or breaches.
- Ownership of physical security and asset management fraud and corruption- related risks (with CRO).
- Manages DA's Information Security in accordance with relevant policies and procedures, including acceptable use of technology and social media (with CRO).

Chief People Officer (CPO)

- Implements and oversees completion of Fraud and Corruption Awareness Training.
- Ensures background checks such as police checks, verification of qualifications/licences, reference checks and, where relevant, Working With Children Checks are conducted as a standard part of all recruitment.'
- Oversees disciplinary processes and outcomes.
- Ensures incentives and performance indicators account for fraud and corruption risks.

Fraud

Fraud is dishonest activity causing actual or potential gain or loss to any person or organization including theft of money or other property by persons internal and/or external to the organization and/or where deception is used at the time, immediately before or immediately following the activity.

The concept of fraud within the meaning of this document can involve fraudulent conduct by internal and/or external parties targeting DA or fraudulent or corrupt conduct by DA itself targeting external parties.

Property in the context of fraud also includes intellectual property and other intangibles such as in formation. 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. [1]

Examples of fraud include (but are not limited to), inflation of invoices, kickbacks, facilitation payments or gifts and foreign bribery and corruption.

Corruption

Corruption is dishonest activity in which a person associated with DA (e.g. director, executive, manager, employee or contractor) acts contrary to the interests of DA and abuses their position of trust in order to achieve personal advantage or advantage for another person or organization. This can also involve corrupt conduct by DA, or a person purporting to act on behalf of and in the interests of DA, in order to secure some form of improper advantage for DA either directly or indirectly.

While conduct must be dishonest for it to meet the definition of corruption, the conduct does not necessarily represent a breach of the law. All acts of bribery are also a form of corruption.[2]

DA prohibits the making of facilitation payments. Workforce and contractors are encouraged to resist all requests to make facilitation payments.

In relation to undertaking work for Commonwealth agencies, corruption is conduct that does or could compromise the integrity, accountability or probity of public administration.

This includes any conduct of any person (whether or not a staff member of a Commonwealth agency) that adversely affects, or that could adversely affect, either directly or indirectly:

- The honest or impartial exercise of any staff member's powers as a staff member of a Commonwealth agency; or

[1] Definition as per the Australian Standard for Fraud and Corruption Control (AS8001-2021).
[2] Ibid.

- The honest or impartial performance of any public official's functions or duties as a public official;
    - Any conduct of a staff member of a Commonwealth agency that constitutes or involves a breach of public trust;
    - Any conduct of a staff member of a Commonwealth agency that constitutes, involves or is engaged in for the purpose of abuse of the person's office; and
    - Any conduct of a staff member of a Commonwealth agency, or former staff member of a Commonwealth agency, that constitutes or involves the misuse of information or documents acquired in the person's capacity as a staff member of a Commonwealth agency.

Corruption may be criminal or non-criminal in nature and may affect any aspect of public administration. For example, an official being offered or accepting a bribe, or engaging in fraud against the entity.[3]

Conflicts of Interest (COI)

Conflict of interest (COI) refers to a conflict between DA's interest and the personal interests of a person in the Workforce that improperly influences the person in the Workforce in the performance of their duties (a real or actual conflict) or has the potential to become a conflict of interest (potential conflict). An apparent or perceived conflict of interest occurs where it appears that a person in the Workforce's personal interests could improperly influence the performance of their duties but this is not in fact the case.[4]

Conflicts of Interest in themselves do not usually constitute corrupt conduct. However, corrupt conduct can arise when a COI is concealed, understated, mismanaged or abused. While having a COI is not necessarily wrong, employees should avoid being placed in conflicting situations where it is practical to do so.

Some examples of the types of situations in which a conflict of interest might arise are:

- Close and/or personal relationships
- Direct reporting and employment arrangements
- Purchasing and procurement activities
- Accepting gifts and benefits (refer to Gifts, Benefits and Hospitality)
- Disclosure of confidential information for personal profit or advantage
- Interests held by a family member or close associate
- Memberships with political, professional, sporting, social or cultural organisations

All Workforce have a responsibility to:

- Report actual, potential or perceived conflicts of interest to their manager when they first become aware, and complete the COI Declaration and Management Plan, and

[3] Definition as per the National Anti-Corruption Commission Act 2022.
[4] Definition from the Australian Public Sector Code of Conduct and DA's Code of Conduct Policy.

- Self-report any changes in circumstances that relate to declared and undeclared conflicts of interest.

COI Declaration and Management Plans for the Workforce (except Board Directors) are captured in a COI Register. The COI Register is accessible to the CRO and CGLR. Board Director COI are declared to the Company Secretary according to DA Board processes.

Gifts, Benefits and Hospitality

A gift, benefit or hospitality under this policy is something that has a monetary value or worth, or other advantage as a result of a business-related relationship.

- Nominal gifts, benefits or hospitality are valued at under $100 and may be accepted and offered, provided that they are not offered on a regular basis.
- Reportable gifts, benefit or hospitality are valued at $100 or greater in value. This also includes any associated travel that may be provided.

The level of approval required for reportable gifts, benefit or hospitality is variable depending on the value of the gift:

- $100 - $250: Line manager approval
- $250-$500: ELT member approval
- $500 - $5000: GCEO approval
- $5000+ and GCEO gifts: Board Chair approval, copied to People and Culture Committee (PCC) Chair and Company Secretary

In all cases, approval is required prior to accepting or offering the gift, benefit or hospitality.

If approval is granted, the DA employee must complete DA's Staff Reportable Gift Declaration Form. Once completed, the form is sent to the relevant manager to confirm approval and is then recorded in DA's Staff Reportable Gifts Register.

Definitions

Brand monitoring service	A Third Party actively monitors websites, social media, marketplaces, and app stores, and takes enforcement action—including takedowns—to remove harmful or infringing content, including domain monitoring, fake ads, fraudulent listings, and executive impersonation.
Facilitation Payment	A minor unofficial payment made to a foreign public official for the purpose of speeding up routine government action.
Personal Information[5]	Information, or an opinion, that could identify an individual or is reasonably identifiable in the circumstances. Personal information may include: • an individual's name, signature, address, phone number or date of birth • sensitive information • credit information • employee record information • photographs

[5] Definition from OAIC https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-personal-information

	• internet protocol (IP) addresses • voice print and facial recognition biometrics (because they collect characteristics that make an individual's voice or face unique) • location information from a mobile device (because it can reveal user activity patterns and habits
Public Interest Disclosure	Public Interest Disclosure Act 2013 (PID Act) provides for the protection of whistleblowers and witnesses. Current and former Workforce are captured under the PID Act where the subject matter of a disclosure directly or indirectly relates to contracted services for the Commonwealth or a contract with the Commonwealth.
Qualified Investigator	A person holding qualifications such as Certificate IV in Government Investigations, or equivalent, and the requisite experience to undertake fraud investigations.
Sensitive Information[6]	Personal information that includes information or an opinion about an individual's: • racial or ethnic origin • political opinions or associations • religious or philosophical beliefs • trade union membership or associations • sexual orientation or practices • criminal record • health or genetic information • some aspects of biometric information. Generally, sensitive information has a higher level of privacy protection than other personal information.
Whistleblower	A whistleblower is someone with inside knowledge of an organisation who reports misconduct or dishonest or illegal activity that may have occurred within that organisation. Protections are provided to whistleblowers to enable them to come forward to report misconduct without fear of retribution or personal detriment under the Corporations Act 2001(Cth).
Workforce	Include the following: • The DA Board • All employees of DA, whether permanent, casual, full-time, part-time, or trainees • Volunteers and work experience placements • Entities or persons providing goods and services to DA (that is contractors and subcontractors)

Acronyms

Cth	Commonwealth
DA	Diabetes Australia (ABN: 47 008 528 461) and its related bodies corporate as defined under the Corporations Act
PID	Public Interest Disclosure

[6] Definition from OAIC https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-personal-information

Additional References

Legislation and Regulations

- Commonwealth Fraud and Corruption Control Framework 2024
- The Fraud and Corruption Control Rule (section 10 of the Public Governance, Performance and Accountability Rule 2014);
- Public Interest Disclosure Act (2013)
- Corporations Act 2001
- National Anti-Corruption Commission Act 2022 (NACC Act)
- Australian Charities and Not-for-profits Commission Act 2012 (Cth) (ACNC Act)
- Australian Charities and Not-for-profits Commission Regulations 2022 (Cth) (ACNC Regulations).

Standards and Codes

- The Australian Standard for Fraud and Corruption Control (AS8001-2021)
- Commonwealth Supplier Code of Conduct

Internal controlled documents

- Code of Conduct Policy
- Whistleblower Policy
- Enterprise Risk Management Policy
- Misconduct and Serious Misconduct Procedure
- Fraud and Corruption Risk Register and Plan
- Fraud & Corruption Response Procedure
- Conflict of Interest Procedure [DRAFT]
- Information Security Policy
- Information Security Management Policy
- Information Access and Control Policy
- Information Security Agreement Procedure
- Information Security Classification and Handling Policy
- Physical Security Standard and Policy
- Workplace Surveillance Policy.