

GOV-008  
Enabling Services

# Financial Crime Policy

Global  
Policy Owner: Legal, Governance, Risk & Compliance Director

---

## 1. PURPOSE

The Fred Hollows Foundation is committed to promoting and adhering to the highest standards of probity and accountability in its governance and operations. The Foundation takes a Zero Tolerance approach towards cases of Financial Crime in its activities and operations within the organisation and under its projects and programs. This Policy sets out the principles and commitments to guide that approach. The Foundation follows the Australian Government's Department of Foreign Affairs and Trade's (DFAT) Fraud and Corruption Control guidelines to prevent, detect, and respond to fraud and corruption in its activities. We are committed to complying with all applicable Anti-money Laundering (AML) and Counter-Terrorism Financing (CTF) laws and implementation of a risk-based AML/CTF program accordingly.

This Policy is managed by The Foundation's Finance and Audit Committee, which holds responsibility for oversight of financial crime matters that occur within or relate to The Foundation.

## 2. SCOPE AND DEFINITIONS

This Policy applies to The Foundation and its subsidiary entities' workplaces and projects globally. Where local law is stricter than this Policy, such local law shall prevail. Circumvention and the attempt to circumvent the provisions of this policy are prohibited. Financial Crime includes Fraud, Corruption, Terrorism Financing, Money Laundering, or violation of Sanctions, otherwise in this Policy capitalised terms have the meaning set out at [paragraph 8](#).

## 3. GUIDING PRINCIPLES

3.1. The guiding principles of this Policy that underpin all of The Foundation's functions, actions and decisions regarding Financial Crime are as follows:

- 3.1.1 We recognise that Financial Crime and in particular Corruption erodes trust, weakens democracy, hampers economic development, and further exacerbates inequality, poverty, social division, and the environmental crisis.
- 3.1.2 We promote a Zero Tolerance culture towards Financial Crime.
- 3.1.3 We implement systems to identify and record Financial Crime risk and prevent and detect incidents of Financial Crime.
- 3.1.4 We educate and train Personnel and partners on how to identify and report Financial Crime.
- 3.1.5 We encourage Personnel, partners, suppliers, and others to speak-up when they suspect Financial Crime.
- 3.1.6 We provide support to all who report cases of Financial Crime, including Whistleblowers.
- 3.1.7 We provide leadership and clear roles and responsibilities with regards to promoting and enforcing a culture of Zero Tolerance towards Financial Crime, including investigation as appropriate and the application of consequences if allegations are proven.
- 3.1.8 We acknowledge Financial Crime and in particular Corruption is a criminal offence and that many countries also have laws that look beyond their own borders to prohibit Bribery abroad.

---

### References

## 4. COMMITMENTS UNDER THIS POLICY

### 4.1. Awareness and training

- 4.1.1 The Foundation is committed to ensuring that Personnel and Implementing Partners:
- (a) are aware of the types of Financial Crime that might occur in their areas of responsibility;
  - (b) are alert for any indication of Financial Crime or improper activity; and
  - (c) maintain controls to avoid such occurrences, including screening to support countering of Terrorism Financing and other financial procedures.
- 4.1.2 Managers are required to ensure that all staff under their supervision are given a copy of this Policy in a language they can understand and acknowledge its receipt. If a written translation is not possible for those who do not speak English, then the Manager must give the person a detailed verbal briefing and take and retain a signed verification from the person that this was done.
- 4.1.3 Managers should also ensure that all staff under their supervision are encouraged to report suspected Financial Crime or vulnerability to Financial Crime. The Foundation will provide regular training to Personnel and Implementing Partners on potential areas of Financial Crime and on mitigation and control measures.

### 4.2. Bribery, Corruption and Facilitation Payments

- 4.2.1 The Foundation is committed to operating without Corruption, including Facilitation Payments and other Bribery.
- 4.2.2 Subject to 4.2.3 - 4.2.4, it is prohibited for The Foundation, its Personnel and Implementing Partners to participate in any Corruption including the offer or receipt of any form of Bribery. All forms of Corruption must be resisted.
- 4.2.3 The Foundation acknowledges that in certain circumstances resisting a request for a Facilitation Payment, a form of Bribery, can create a serious threat to life or safety. In such cases safety to people comes first.
- 4.2.4 If asked to make a Facilitation Payment, Personnel should:
- (a) always resist making the payment if it is safe to do so;
  - (b) if the request is accompanied by threats to safety, make the payment and when safe record the details, for example location, name and role of requester, date and amount;
  - (c) report the matter to your manager and The Foundation's Financial Crime Officer or [speak-up@hollows.org](mailto:speak-up@hollows.org) as soon as possible and always the same day.
- 4.2.5 If resisting a Facilitation Payment is likely to cause significant disruption to the delivery of a Foundation project or service, all Personnel should resist payment but immediately notify their manager and The Foundation's Financial Crime Officer so that appropriate action may be considered.

### 4.3. Controls, monitoring of transactions and audit

- 4.3.1 The Foundation commits to a robust framework which prevents, deters, and detects Financial Crime and will put in place appropriate controls and procedures, such as a Finance Manual, to achieve this commitment.
- 4.3.2 It is the responsibility of all Personnel to adhere to these controls and procedures, carrying out their work in such a way as to prevent Financial Crime in all forms occurring in the workplace.
- 4.3.3 These controls will include regular monitoring of transactions and the engagement of internal and external audit professionals.

---

#### References

#### 4.4. Third party risk

- 4.4.1 Recognising the risk raised by third parties, The Foundation commits to screening, on an ongoing basis, all Personnel, partners and suppliers against appropriate money laundering, counter terrorism financing and sanctions lists
- 4.4.2 The Foundation commits to conducting due diligence on Implementing Partners using a risk-based approach, including additional requirements for moderate to high-risk contexts
- 4.4.3 All grants to Implementing Partners or other third parties must be transparent. The recipient's identity and planned use of the grant must be clear and the reason and purpose for the grant must be justifiable, approved as per The Foundation' Delegation Policy and documented in accordance with The Foundation's contract management process.

#### 4.5. Reporting, confidentiality and protection

- 4.5.1 Employees must also be alert for occurrences of Financial Crime, be aware that unusual transactions or behaviours could be indications of Financial Crime and report potential cases of Financial Crime as outlined in section 5.
- 4.5.2 The Foundation commits to absolute confidentiality and fairness in all matters raised under this Policy.
- 4.5.3 Whistleblowers making a report in accordance with this Policy will be protected from detriment and may make their report confidentially in accordance with the Speak-Up Policy.
- 4.5.4 Any suspected Corrupt conduct in DFAT-funded activities will be reported to DFAT and relevant authorities (e.g. NACC) as required.
- 4.5.5 All files and records created from an investigation under this Policy will be retained under strict security.

#### 4.6. Gifts & Hospitality

- 4.6.1 The Foundation commits to not provide any undue advantages to decision-makers, their associates, or their family members.

The Foundation will not offer gifts to decision-makers and any hospitality offered must be reasonable, bona fide, and socially acceptable, not allowing for any impression of improper influence over the administrative process or the execution of their professional duties.

- 4.6.2 The Foundation will not accept any gift or hospitality, entertainment, loan or anything else of value from any organisation or individual if it could be reasonably construed or perceived that the gift is motivated by a wish to influence The Foundation.

Gifts valued above AUD50, whether offered or received, must be disclosed by registration on [The Foundation's Gifts, Hospitality & Political Event Register](#). Gifts valued above AUD100 must have the prior approval of the relevant Director. Gifts valued above AUD200 must have the approval of the CEO.

- 4.6.3 The Foundation will only invite appropriate stakeholders to events and on fact-finding trips, subject to the informative purpose being clearly evident. Only reasonable food and accommodation may be offered, and no hosting or travel of accompanying guests will be covered by our organisation (other than for support purposes, such as disability or cultural).

The Foundation will not provide any donation or other form of contributions to political parties, whether financial or in-kind. For the avoidance of doubt, this does not prohibit The Foundation making payments to political parties for general attendance at events that advance The

---

#### References

Foundation's advocacy efforts. To ensure transparency all Personnel making such payments should also be included in the register.

## 5. REPORTING SUSPECTED FINANCIAL CRIME

### 5.1. Financial Crime investigations

- 5.1.1 To report suspected Financial Crime, refer to the Financial Crime Concern Reporting Process at Annexure 1.
- 5.1.2 To report suspected Financial Crime and identify as a Whistleblower please refer to the [Speak-Up Policy](#) or email [speak-up@hollows.org](mailto:speak-up@hollows.org) / call or text +61 418 814 609.
- 5.1.3 The Foundation will assess all concerns raised and instigate a fair and impartial response as appropriate.

### 5.2. Actions arising from Financial Crime investigations

#### Disciplinary procedures

- 5.2.1 Persons who are deemed to have committed a Financial Crime will be dealt with in accordance with The Foundation's disciplinary procedures.
- 5.2.2 Proven allegations of Financial Crime will result in immediate dismissal, or in the case of an Implementing Partner or supplier immediate contract termination. Alternative disciplinary action can only be taken with the approval of the CEO. If the matter relates to the CEO this approval must be from the Board.
- 5.2.3 Where appropriate, The Foundation may refer significant Financial Crime to the police or appropriate relevant authorities. In every case, the final decision regarding whether to make such a referral rest with the CEO or the Board if the matter involves the CEO.

#### Changes to systems or controls

- 5.2.4 The investigation may highlight where there has been a failure of supervision and / or a breakdown or absence of control. The course of action required to improve systems should be documented in the investigation report and implemented as soon as possible.

#### Recovery of losses

- 5.2.5 Where The Foundation has suffered loss, full restitution will be sought of any benefit or advantage obtained and the recovery of costs may be sought from individuals or organisations responsible for the loss.
- 5.2.6 If the individual or organisation cannot or will not make good the loss, consideration will be given to taking civil legal action to recover losses. This is in addition to any criminal proceedings which may result.

## 6. RESPONSIBILITIES & ACCOUNTABILITIES

### 6.1. Board

The Board of The Foundation is responsible for:

- 6.1.1 creating a culture of Zero Tolerance toward Financial Crime at The Foundation;
- 6.1.2 providing governance guidance for The Foundation in relation to Financial Crime; and
- 6.1.3 approving this Policy.

### 6.2. Chief Executive Officer

- 6.2.1 The CEO is responsible for ensuring this Policy is upheld and will inform the Board of any concerns relating to Financial Crime that may present risk to The Foundation, its Personnel, beneficiaries, partners, reputation, operations, or other activities.

---

#### References

- 6.2.2 The CEO will ensure progress in relation to combatting Financial Crime across The Foundation, including Terrorism Financing, is included in standard reporting to The Board.
- 6.2.3 The CEO will hold relevant Senior Leaders accountable to this Policy.

### **6.3. Senior Leaders**

- 6.3.1 The Legal, Governance, Risk & Compliance Director will promote the existence of this Policy to all Personnel.
- 6.3.2 Senior Leaders will ensure Foundation and Divisional procedures, practices, plans, and operations align with this Policy and that all relevant Personnel are aware of, and understand, this Policy and their responsibilities under it.
- 6.3.3 Divisions are encouraged to put in place procedures to implement the principles set out in this Policy; including for specific countries. However, this Policy will prevail to the extent of any ambiguity or inconsistency between this Policy and those procedures.
- 6.3.4 Senior Leaders are responsible for monitoring and responding to any Financial Crime risk or concerns arising within The Foundation's business activities. The Senior Leaders will include risks and incidents on the relevant registers and seek the advice of the Policy Owner on issues of contention.

### **6.4. Policy Owner**

- 6.4.1 The Policy Owner is responsible to ensure the Policy complies with The Foundation's obligations and contemporary practice and will update this Policy as required.
- 6.4.2 The Policy Owner will be responsible for addressing any issues arising in relation to this Policy and will be or arrange a point of contact for all Personnel for any issue of contention.
- 6.4.3 The Policy Owner will assist the CEO prepare the reporting set out in 6.2.2.
- 6.4.4 The Policy Owner will inform the CEO of any key risk to The Foundation regarding Financial Crime and will record risks and incidents on the relevant organisational register.

### **6.5. Managers (Country and People Managers)**

- 6.5.1 Managers will demonstrate a commitment to Zero Tolerance of Financial Crime and model best practices.
- 6.5.2 Managers are to communicate this Policy and all related procedures to Personnel including ensuring that Financial Crime is a standard agenda item at all regular team meetings.
- 6.5.3 Managers will engage with their teams in an open, honest, and meaningful way to ensure they understand what is expected of them.
- 6.5.4 Managers will constructively participate in the resolution of issues relating to Financial Crime.

### **6.6. All Personnel**

- 6.6.1 All Personnel will adhere to the principles and commitments under this Policy and any related procedures and will take all reasonable care to ensure that their actions or omissions are not in breach of this Policy nor directly or indirectly encourage others to breach this, Policy.
- 6.6.2 All Personnel are responsible for identifying and responding to any Financial Crime-based risk or concerns arising within The Foundation's business activities. Any matters of contention must be reported to the relevant Executive Director.
- 6.6.3 If Personnel have any doubts or concerns as to whether a specific behaviour is allowed or not or has any other questions in relation to this Policy, they should contact the Financial Crime Officer, Safeguarding Officer or Global General Counsel to seek clarification. This can be arranged confidentially.

---

#### References

## 6.7. All associated stakeholders

All associated stakeholders operating with or on behalf of The Foundation are responsible to understand and abide by the principles and relevant commitments under this Policy and to advise the primary contact point within The Foundation of any issues that may arise.

## 7. MONITORING

- 7.1. A report on the implementation of this Policy will be submitted to the Board no less than every three years across The Foundation's business activities, including the countries in which we work. The Policy Owner is responsible for compiling this report and submission to the CEO.
- 7.2. This Policy will be reviewed every three years and the Policy Owner is responsible to undertake this review.
- 7.3. The Enabling Services Division has oversight for all Governance and Operational Policy and will ensure the Policy is listed on the Policy Register and provide support to the Policy Owner to ensure monitoring and reporting obligations are met.

## 8. DEFINITIONS

**Advantage** means any economic and non-economic advantage of any kind improving the receiver's situation and to which the receiver is not legally entitled, including gifts, meals, entertainment, travel and lodging.

**Bribery** is the offering, promising, giving, accepting, or soliciting of an Advantage as an inducement for an action which is illegal, unethical or a breach of trust. Inducements can take the form of gifts, cash, loans, fees, Facilitation Payments, rewards or other Advantages.

**Collusion** A secret agreement between parties, in the public and/or private sector, to conspire to commit actions aimed to deceive or commit fraud with the objective of illicit financial gain. The parties involved often are referred to as cartels. It includes but is not limited to the following:

- (a) Agreeing to increase prices faced by consumers and/or partners.
- (b) Deals between suppliers and customers. For example, price fixing or inflation of prices.
- (c) Monopoly pricing, which refers to a market situation when there is a single buyer of a commodity or service.
- (d) Price fixing where rival companies come to an illicit agreement not to sell goods or services below a certain price.
- (e) Agreement between existing partners in an industry to exclude new organisations from deals to prevent the market becoming more competitive.
- (f) Collusive tendering, for example 'cover prices' for competitive tendering in bidding for public construction contracts. This is when rival organisations agree to set artificially high price to allow the firm of choice to win with a relatively high contract offer.

**Conflict of Interest** Situation where an individual or the entity for which they work, whether a government, business, media outlet or civil society organisation, is confronted with choosing between the duties and demands of their position and their own private interests.

**Corruption** is the abuse of entrusted power for private gain. Corruption includes but is not limited to:

- (a) Bribery;
- (b) Favouritism;
- (c) Extortion; and
- (d) Collusion.

**Extortion** is the act of utilising, either directly or indirectly, one's access to a position of power or knowledge to demand unmerited cooperation or compensation as a result of coercive threats.

**Facilitation Payments** means a small bribe, also called a 'facilitating', 'speed' or 'grease' payment made to a Public Official to secure or expedite the performance of a routine or necessary action to which

---

### References

the payer has legal or other entitlement. Facilitation payments can be distinguished from other bribes as they are not in any way linked to securing any decision to award, continue or create new business.

**Favouritism** is favouring of one person or group at the expense of others and includes nepotism, which is favouritism shown to relatives.

**Financial Crime** refers to activities related to any of the following:

- (a) Fraud;
- (b) Corruption;
- (c) Terrorism Financing;
- (d) Money Laundering; or
- (e) violation of Sanctions.

**Financial Crime Officer** means the Head of Risk, Integrity & Safety of The Foundation, or such other person appointed by the Legal, Governance, Risk & Compliance Director to be accountable for the management of financial crime.

**Fraud** means dishonestly obtaining a benefit, or causing a loss, by deception or other means. In this definition, benefit refers to both tangible items, such as money or objects, and intangible benefits including power, status, or information. Fraud includes but is not limited to the following:

- (a) theft of funds or any other of The Foundation's property;
- (b) falsification of costs or expenses;
- (c) forgery or alteration of documents including invoices;
- (d) unauthorised destruction or removal of records;
- (e) inappropriate personal use of The Foundation's assets;
- (f) seeking or accepting cash, gifts or other benefits from third parties in exchange for preferment of the third parties in their dealings with The Foundation;
- (g) paying of excessive prices or fees to third parties with the aim of personal or organisational gain;
- (h) using an electronic signature without the written consent of the owner; and
- (i) failure to declare a Conflict of Interest.

**Implementing Partners** means an organisation who has a financial partnership agreement with The Foundation to implement the work that we do.

**Money Laundering** means the process of concealing the origin, ownership, or destination of illegally or dishonestly obtained money, including Virtual Assets, and hiding it within legitimate economic activities to make them appear legal.

**NACC** means the Australian National Anti-Corruption Commission.

**Personnel** means any person who carries out work in any capacity for the benefit of The Foundation or its related bodies corporate, which includes employees, contractors, sub-contractors, consultants, work experience students, volunteers, Board directors and any other person who formally acts on The Foundation's behalf.

**Public Official** has the meaning given under local law but will generally include employees and contractors of the government and government bodies. The Foundation otherwise adopts the definition of Foreign Public Official in the Australian Criminal Code Act 1995. Please see the General Counsel for more guidance.

**Safeguarding Officer or SO** means the person appointed by the CEO to be accountable for the management of safeguarding at The Foundation globally.

**Sanctions** means measures not involving the use of armed force imposed in situations of international concern, including the grave repression of the human rights or democratic freedoms of a population by a government, or the proliferation of weapons of mass destruction or their means of delivery, or internal

or international armed conflict, including under the Charter of the United Nations Act 1945, the Australian Autonomous Sanctions Act 2011 (Cth) or other local legislation as applicable.

**Speak-Up Policy** means The Foundation’s policy on complaints and whistleblowing: [ORG-010 Speak-Up Policy](#).

**Terrorism Financing** means intentionally providing or collecting funds and being reckless as to whether those funds would be used to facilitate or engage in a terrorist act.

**Virtual Asset:** A digital representation of value regulated under the amended AML/CTF Act (2024), including cryptocurrency exchanges, custodial wallet providers, ICO/ITO issuers, and other virtual asset service providers.

**Whistleblower** has the meaning given to that term in the Speak-Up Policy.

**Zero Tolerance:** means that consequences will apply if allegations are proven. A zero-tolerance approach to Financial Crime does not mean that all Financial Crime can be avoided or prevented. Instead a zero- tolerance approach represents a set of principles and commitments that are applied by The Foundation to prevent, detect, investigate, and respond to Financial Crime in order to effectively manage associated risks.

## CONTROL OF DOCUMENTATION

<b>Document Number</b>	GOV-008		
<b>Document Name</b>	Financial Crime Policy		
<b>History</b>	Revised to align with updates to DFAT guidance and the introduction of the NACC.		
<b>Date Created</b>	1/06/2007		
<b>Author(s)</b>	Finance Director & Head of Program Finance		
<b>Master document location</b>	FredNet		
<b>Policy owner(s)</b>	Legal, Governance, Risk & Compliance Director		
<b>Division</b>	Enabling Services		
<b>Review Body</b>	Finance & Audit Committee		
<b>Approval Body</b>	Board		
<b>Version Date</b>	4/03/2026	<b>Version Number</b>	1
<b>Next review date</b>	3/03/2029	<b>Review Period</b>	3 years
<b>Related Policies</b>	GOV-006 Speak-Up Policy; GOV-004 Safeguarding People Policy; GOV-010 Conflict of Interest Policy; Internal Audit Charter; OPR-005 Procurement Policy		

---

### References

## ANNEXURE 1 – FINANCIAL CRIME CONCERN REPORTING PROCESS AND FORM

### Part A – Financial Crime Concern Reporting Process

1. Any Personnel or Representatives of The Foundation that become aware of or suspected financial crime within the activities of The Foundation, our Partners or otherwise while at work or any other breach of the Financial Crime Policy must immediately notify The Foundation's Safeguarding Officer (SO) ([speak-up@hollows.org](mailto:speak-up@hollows.org) / +61 418 814 609).<sup>1</sup>
2. Part B sets out the Financial Crime Concern Reporting Form. Partners must notify either the SO directly or their partner relationship manager at The Foundation. No other staff from The Foundation or external party should be informed without the express written consent of the SO.
3. The SO will notify the CEO, Financial Crime Officer (**FCO**) and Global General Counsel (GGC)<sup>2</sup> immediately.
4. If the concern or allegation relates to activities receiving institutional funding, the CEO will inform the institutional Donor. For example, for DFAT this is within 5 working days. Other Donor and Partner notification requirements including FCDO and USAID should also be checked case by case and followed strictly.<sup>3</sup>
5. The SO, CEO, GGC and FCO will jointly consider the nature of the alleged offence, and decide on the next steps, including any further action including need for suspension. Next step action may involve an investigation led by The Foundation's Director of People & Organisational Development, the FCO or an external expert depending on the nature of the Financial Crime Concern.
6. The GGC will support the SO and FCO to ensure that relevant laws are followed in relation to investigation, reporting and sanctions including that if the alleged incident is a breach of law the SO and FCO will report it to the relevant authorities. For example, in Australia this would be by the SO to the Australian Federal Police. In other countries the CM will support the GGC to determine the appropriate authority.
7. The SO, working with the GGC and FCO where relevant, will inform the relevant stakeholders of the result of the investigation. This may include the person who made the report and the person against whom the allegation was made against, if relevant.
8. The CEO will keep the institutional Donor apprised of developments as appropriate.
9. The SO and FCO will ensure that the fact a Financial Crime Concern has been raised is included in relevant registers and in reporting presented to Board.
10. If any allegations are made suggesting that The Foundation itself as an organisation has committed an offence under any laws, then the SO must refer the allegation to the GGC who will advise the CEO and/or the Board as appropriate in the circumstances

---

<sup>1</sup> If the allegation is about the CEO, the report should be escalated by the SO to the Chair of the Board, if the SO, the report should go to the CEO who will inform the FCO in lieu of the SO (for others the CEO / SO will substitute as needs).

<sup>2</sup> No later than same day. Given the nature of the investigations, GC may ask external specialised counsel to advise.

<sup>3</sup> An overview of Donor requirements is available from the Grants team

---

#### References

**Part B - The Fred Hollows Foundation Financial Crime Concern Reporting Form**
**ALL INFORMATION IN THIS FORM WILL BE TREATED CONFIDENTIALLY**

Personnel, Representatives and Partners must report any suspected financial crime and any instances of the Financial Crime Policy non-compliance. You can lodge this form online on FredNet or send to [speak-up@hollows.org](mailto:speak-up@hollows.org).

<b>Information about you</b> (optional if you wish to remain anonymous)	
<b>Name</b>	
<b>Position in FHF or in relation to FHF</b>	
<b>Telephone (include mobile)</b>	
<b>Email</b>	
<b>Date</b>	
<b>Information about suspected Financial Crime</b>	
<b>Country:</b>	
<b>Date and Nature of Incident</b>	
<b>Amount Lost:</b>	
<b>Amount Recovered:</b>	
<b>Description of the suspected financial crime (please provide as much detail as you can on the background of the incident)</b>	
<b>Location of the suspected financial crime:</b>	
<b>How you became aware of the financial crime e.g., controls testing, witnessed it, spot check</b>	
<b>Information about the financial crime</b>	
<b>Name(s) of person (s) that may have committed the suspected financial crime</b>	
<b>If not FHF, name of the organisation/company for whom the person that may have committed the suspected financial crime works:</b>	
<b>In which FHF project?</b>	
<b>Name of the donor who funds this project (if known):</b>	
<b>Any supporting evidence you can share including scanned documents or photos:</b>	
<b>Have you reported this Financial Crime to anyone else either internally at FHF or externally to other bodies e.g., partner or police? If yes, please include details.</b>	
<b>Weakness in process and remedial action taken.</b>	

References