

Table of Contents

Old Mutual South Africa (OMSA) Financial Crime Policy	2
1. Why we need a Policy	1
2. Purpose of this Policy	1
3. Who this Policy Applies to	1
4. GFS Mandate.....	1
5. Employee Responsibilities	2
6. Management Responsibilities.....	3
7. Group Forensic Services (GFS) Responsibilities	3
8. Reporting.....	4
9. Confidentiality	5
10. Suspension	5
11. Disciplinary and/or Legal Action	6
12. Conclusion	6
Annexure A: Fraud, Theft, Corruption, Internal Irregularities, Cybercrime	7
1. Definitions	7
Fraud	7
Annexure B: Conflicts of Interest.....	10
1. Definition	10
2. Disclosure(s)	11
3. Approval	12
4. Decline	12
5. Review Process	12
6. Directors.....	13
Annexure C: Moonlighting	14
1. Approval	14
Application Form.....	14
2. Exceptions to this rule	14
Annexure D: Gifts	15
1. What this Policy covers	15
2. Allowed Gifts	16
3. Gifts not allowed.....	17
4. Gifts to be declared	17
5. Gifts Register	17
6. Approval	17
Annexure E: WhistleBlowing	18
1. What this Policy does <u>not</u> cover	18
2. Concerns that can be raised and reported	18
3. Your protection.....	19

1 July 2011

Old Mutual South Africa (OMSA) Financial Crime Policy

1. Why we need a Policy

Old Mutual (South Africa)'s – (The Company) Code of Ethics requires the Company and employees to act in accordance with legislation at all times and with integrity, to safeguard its reputation and resources (including both tangible and intangible).

The Financial Crime Policy (The Policy) is designed to provide the following:

- Guidance on how employees should behave
- How to report suspected or actual breaches of The Policy
- Process that will be followed once the reports have been received

2. Purpose of this Policy

The policies listed below have been replaced by this Policy which provides information to employees in order to make informed decisions as to how they should interpret the Company's Values.

- Policy on Fraud, Theft, Corruption, Cyber-crime and Associated Internal Irregularities
- Conflicts of Interest Policy
- Moonlighting Policy
- Gifts Policy
- Whistle Blowing Policy

This Policy contains elements of each of the above policies, (eg. Employee and Management responsibilities, reporting, confidentiality and suspension.)

Actual definitions and examples of Fraud, Theft, Corruption, Cyber-crime, Associated Internal Irregularities, Conflicts of Interest, Moonlighting, Gifts and Whistle-blowing are listed in Annexures A – E.

3. Who this Policy Applies to

This Policy applies to all employees (Permanent and Temporary) within The Company (excluding Nedbank and Mutual & Federal) insofar as this Policy is applicable and has been adopted by the subsidiary Boards of the Companies.

4. GFS Mandate

Group Forensic Services (GFS) delivers a centralised, independent, objective and integrated forensic service to the Old Mutual Group and its stakeholders.

This is achieved by providing fraud risk intelligence through its awareness, detection, and investigation functions, in order to enable management to prevent, identify and manage the risk of fraud, theft, corruption, and associated internal irregularities.

The Audit Risk and Compliance Committee (ARCC) of the Board has tasked GFS with the conducting of investigations and fraud risk assessments independently, objectively and without undue influence being exercised in any manner, or by any other party or individual.

5. Employee Responsibilities

All employees have a general duty to act in the best interest of their employer.

This includes reporting suspected incidents of:

- Dishonesty
- Misconduct; or
- Policy breaches

Employees should be able to recognise that unusual events, transactions or dishonest behaviour could lead to Fraud, Theft, Corruption, Cyber-Crime and material breaches of other Processes or Policies involving dishonesty and misconduct. Any employee who is unclear as to what constitutes a breach of a Policy should seek guidance from their Line Manager or Group Forensic Services (GFS).

Employees may be requested to assist GFS when conducting investigations eg.

- To assist in drawing reports or in providing required expertise in resolving technical queries relating to their job function
- They must also make themselves available for interviews and consultations in a timely manner at a venue reasonably determined by GFS

Providing unrestricted access to the following under their control:

- Their workspace where that is situated on company premises
- Company documents, electronic data, electronic artifacts and other records
- Company computers, printers, facsimile machines and other electronic devices such as company mobile telephones, mobile storage devices, and Blackberry-type devices
- Electronic user devices that are attached to company computers, printers, or facsimile machines.

An employee has the right to refuse to provide answers to particular questions that may amount to an admission of guilt to a criminal offence. This refusal will result in findings and recommendations to Management being based on available information.

Where an employee:

- Intentionally obstructs GFS in the conduct of investigations, or
- Deliberately misleads GFS, or
- Knowingly provides false information to GFS,

GFS may make recommendations to management regarding the suspension of the employee during the course of the investigation.

Searches

A search should take place only if a reasonable suspicion of an irregularity exists and should not disregard the employee's competing right to privacy.

- All employees may be subject to searches of their belongings, clothing or vehicle, when on company controlled premises
- Any suspicious object may be seized and stored pending further investigation

6. Management Responsibilities

Investigative work performed by inexperienced individuals may jeopardise the outcome of the investigation. Management must ensure that:

- They do not conduct their own investigations beyond that needed to establish a reasonable suspicion, unless this has been agreed with GFS in advance
- They immediately report all suspected breaches of these Policies as soon as they have a reasonable suspicion that such an incident has occurred
- Internal controls which assist with the prevention, detection and investigation of unethical behaviour are in place and operating effectively
- All employees are made aware of all the Company Policies
- GFS is given timely and unrestricted access to all Company functions, records, property and employees
- The necessary assistance and co-operation is provided to GFS
- All recommendations by GFS including the suspension of employees pending the outcome of an investigation are considered and responded to
- The drafting of appropriate charges, initiating and convening of disciplinary hearings takes place

Managers do not have any authority over any decision by GFS:

- To conduct an investigation
- Nor to influence the scope, timing, methodology or direction of investigations
- Nor do they have the right to change the contents of the reporting of the results or recommendations of investigations

Note:

In matters of a particularly complex or serious nature the Head of GFS, in consultation with the Chief Internal Auditor of The Company, has the discretion to draft misconduct charges and appoint an appropriate presenter for a misconduct hearing.

7. Group Forensic Services (GFS) Responsibilities

GFS is committed to investigating all Fraud, Theft, Corruption, Cyber-Crime and material breaches of other Processes or Policies involving dishonesty and misconduct in independent and objective manner. GFS will also:

- Where appropriate, consult with relevant stakeholders
- Conduct all our work in accordance with applicable Laws
- Determine the scope and priority of all investigations
- Decide who will be responsible for conducting investigations
- Report to, and liaise with, the relevant law enforcement authorities
- Report on the progress and outcomes of investigations to Managers
- Make appropriate recommendations for possible further action

Where GFS deems it necessary:

- It is entitled to conduct surveillance,
- To intercept, monitor and retrieve email communications, record telephone conversations and related investigation activities

8. Reporting

8.1 Reporting a concern internally

Option 1

You may raise the matter directly with Group Forensic Services (GFS):

Indicate if you are willing to reveal your identity to GFS or if GFS is permitted to reveal your identity for the purposes of the investigation.

General contact details	Head Office, Block 4F, Mutualpark (021) 509 7012	For a direct or telephonic consultation
	93 Grayston Drive, Sandton (011) 217 1797	
	19th Floor, Durban Bay House, 333 Anton Lembede Street, Durban, 4001 (031) 369 8509 / 8510	
Email	gfs@oldmutual.com	To email a completed

Option 2

You may raise the concern anonymously by contacting the independent reporting line, Tip-offs Anonymous (TOA).

- TOA will ensure that you remain anonymous by removing all information that might link you to the report, before forwarding the information to GFS for investigation.
- If however you still have concerns about your identity being disclosed, we suggest that you contact TOA from facilities outside of Old Mutual.

The report you make to TOA will never reveal your identity or your gender, unless you inform them that you are happy that your identity may be forwarded to GFS.

Reporting anonymously via the independent Tip-offs Anonymous process:

Free Call phone	0800 222 117	For a telephonic consultation
Free Call fax	0800 00 77 88	For the sending of relevant documentation to support your report
Unique e-mail	oldmutual@tip-offs.com	E-mails will also remain anonymous since they will be relayed through a server that "removes" your name as sender as well as all other source information
Free Post address	Tip-offs Anonymous, Freepost DN 298, Umhlanga Rocks, 4320	To which you can mail letters and relevant documentation
Website addresses	www.tip-offs.com www.oldmutualanonymoureports.co.za	To find out more information and make an online report

SMS	32840	Send an sms worded "Please call me" – also include your language and company name. Cost is R1.00 per sms. You will receive an automated response from Deloitte Tip-Offs Anonymous via sms. An agent will contact you.
-----	-------	---

8.2 Reporting a concern externally

If you do choose to make disclosures externally you are required to do so in accordance with the Protected Disclosure Act. Your Legal Advisor, Union Representative or Open Democratic Advice Centre (ODAC) would be able to advise you on this.

The Act only allows you to make external reports under certain circumstances. For example where the concern:

- **Cannot be raised internally because you reasonably believed you would be harassed, victimised, or that the evidence would be concealed or destroyed**
- **Was raised internally via the approved channels but it was not properly addressed**
- **Was exceptionally serious**

You are always encouraged to raise your concerns via the appropriate internal channels first (as set out in this Policy) and to obtain legal advice before raising any matter externally.

9. Confidentiality

All information reported to GFS is confidential and:

- Will not be disclosed or discussed with any other individual other than for the purpose of conducting the investigation
- When necessary, be reported to the appropriate authorities
- May be utilised in disciplinary, legal or other related action

Any individual who:

- Reports
- Provides information
- Is interviewed as part of an investigation

must maintain the confidentiality of that information, and of the investigation.

10. Suspension

GFS may make recommendations to management regarding possible suspensions during the course of an investigation.

Any employee who is under investigation may be suspended, pending the outcome of the investigation.

11. Disciplinary and/or Legal Action

Any breach of this Policy may lead to disciplinary and/or legal action

12. Conclusion

This Policy forms part of the Company Code of Conduct and should be read together with all other policies including any applicable Group Policies.

Annexure A: Fraud, Theft, Corruption, Internal Irregularities, Cybercrime

The Company, persons working for the Company or external third parties can be involved in committing fraud, theft, corruption cyber crime or associated internal irregularities.

1. Definitions

For the purposes of this Policy the following definitions apply.

Fraud

In accordance with the Common Law:

Any unlawful act or omission by which a misrepresentation is made with the intention to defraud which causes actual or potential prejudice to another, whether or not there is personal benefit to the perpetrator.

Examples:

- Misrepresenting client details on a policy application (incorrect income, height, weight etc)
- Submitting a misleading curriculum vitae (CV) when applying for work
- Using someone else's password to access a computer system
- Disclosing client or staff confidential information for financial gain

Theft

In accordance with the Common Law:

The misappropriation of movable property or money with the intention of permanently depriving the owner of the use or possession of these goods (steal).

Example:

- Taking something of value which does not belong to you, without permission from the owner, eg a computer and the information on that computer

Corruption

The Prevention and Combating of Corrupt Activities Act states in Chapter 2 Part 3 that:

Any person who is party to an employment relationship is guilty of an offence when:

1. Receiving an unauthorised gratification* if that person:

- Directly or indirectly
- Accepts/agrees/offers to accept
- From any other person
- Any unauthorised gratification, whether for the benefit of :- that person or another person

2. Offering an unauthorised gratification* if that person:

- Directly or indirectly
- Accepts/agrees/offers to give
- To any person who is party to an employment relationship
- Any unauthorised gratification, whether for the benefit of: - that person or another person

***What is Gratification?**

Examples

- Cash/money
- Donation, gift, loan, fee
- Any right or privilege
- Any payment of any loan or liability
- Any service, favour or advantage
- Any valuable consideration or benefit, eg a free holiday, tickets to a match
- Avoidance of loss, liability, penalty, eg. Pay money you owe in return for a favour eg employ a member of the "payers" family
- Any office, status, honour, employment, eg. Promote you, appoint you into a senior position
- Any forbearance to demand money, (Forbearance means "abstention" from, eg enforcing payment of a debt"
- Any real or pretended aid, vote, consent, influence

Corruption Examples:

- Offering someone who does not work for Old Mutual client information in exchange for a reward (money, other goods or services)
- Intentionally altering an application so that a potential client qualifies for benefits he/she would not qualify for in return for a "reward" (abusing your position of employment to gain an advantage)
- Paying a supplier's relationship manager a 'performance bonus' in exchange for discounted rates
- Excessive provision of gifts and entertainment to government officials in order to generate business

Cyber-crime

Cyber-crime is defined in Chapter 13 of the Electronic Communications Act (ECT) as:

Any unauthorised access, interception or interference with electronic data, computer-related extortion, fraud and forgery, as well as any attempt to commit, assist or encourage these offences.

Example:

- Electronic document forgery
- Electronic hiding of suspicious information
- Modifying or destroying electronic data

Internal Irregularity

This includes acts involving unethical or dishonest conduct and these are committed against the background of:

- The employee's general duty to act in the best interest of the employer
- The employment contract between the employee and employer
- The employee's job description
- The employee's performance contract
- The OMSA Policy framework

Example:

- Abuse or misuse of company property and/or time
- Unacceptable loss of Company assets

Annexure B: Conflicts of Interest

A conflict of interest is when an employee's personal and/or business interests, whether **direct or indirect**, conflict with, or could reasonably be perceived to conflict with, the interests of the Company. This involvement may affect the employee's ability to act with integrity or objectivity in carrying out their role.

1. Definition

What is a Conflict of Interest?

Direct

- Running other businesses in competition with the Company
- Taking on additional employment which materially interferes with the employee's expected performance
- When an employee uses their work position for private gain for themselves, any family member, friends or business associate eg:
 - accessing confidential business information, or
 - involvement in insider dealing or trading, or
 - using company time, materials, property or facilities

Indirect

- Non disclosure of any business interests that members of your family are involved in where that business conducts, or may in the future conduct business with the Company
- Where individuals are principal links in one company, and an employee of Old Mutual, and where one of the other principal links in the company also has links to another company which conducts business with Old Mutual

Principal Link: A principal link brings together the personal details of an individual and any current business interests that the individual may have.

Employee: Includes permanent and temporary employees, independent contractors, vendors, service providers (including their employees).

Employee's Family: Includes all people connected by blood, marriage, adoption and co-habitation.

Nepotism: The employment, promotion or advancement of a family member or relative in a position, where that employee is able to directly or indirectly influence the decisions relating to these actions.

The FAIS Conflict of Interest Policy differs from the Financial Crime Policy definition of Conflicts of Interest as it deals with any situation in which a **provider or a representative** has an actual or potential interest that may, in rendering a financial service to a client:

- Influence the objective performance of their obligations to that client; or
- Prevent a provider or representative from rendering an unbiased and fair financial service to that client, or from acting in the best interests of that client, including but not limited to:
 - A financial interest
 - An ownership interest
 - Any relationship with a third party

2. Disclosure(s)

Every employee must disclose any personal and/or business activities in which they have a **direct or indirect** interest when:

- Income derived from that interest is more than 10% of your Old Mutual Total Guaranteed Package (TGP) in any twelve (12) month period
- They are involved in, or are able to influence, the decision making process on behalf of The Company relating to their personal and/or business activities
- A family member or relative
 - Is employed, promoted or transferred into a position, where that employee is able to directly or indirectly influence the decisions relating to their personal and /or business activities.
 - Reports to you either directly or indirectly
 - Approves, processes, reviews or audits your work

Disclosures in advance, and annual disclosures

Employees must disclose all business interests (including pre-existing arrangements) annually, between 1 to 30 April and when:

- Any negotiations begin with a third party
- Any decision-making process where a conflict of interest may arise
- Previously disclosed interest or activity changes materially

The Company will be able to, via this disclosure process:

- Allow employees to acquire and maintain personal outside interests where appropriate
- Protect employees from false allegations of conflicts of interest

Process

- This process is explained on Groupnet and Gateway, both for office staff and field staff.
- The process for Directors, EXCO members and employees whose Role Size falls in the R,S,T,U range is communicated via e-mail in April of each year. A disclosure must be made whether a conflict of interest exists or not i.e. a nil return must be submitted certifying that they understand the policy and that

- they have no conflicts to disclose.
- Declarations by Board Members in terms of the Companies Act should be submitted to the Company Secretary, and should be kept up to date. This process is managed by Group Risk in consultation with the Company Secretary.

3. Approval

- The following must be recorded on Oracle
- Approval of this interest or activity
 - The conditions of approval
- The employee applying for approval may not commence the activity prior to the activity being approved.

4. Decline

- Where the interest or activity that gives rise to the potential conflict of interest:
- Is judged to be inappropriate or
 - Has the potential to damage Old Mutual’s interests and/or reputation
- The activity should be declined and recorded on Oracle HRMS.

5. Review Process

- Employees have the right to request a single review of the decision where the activity or interest is declined, or where conditional approvals are granted
- The request must be in writing including the reasons for the request, and copies of all documents relating to the original disclosure of the activity or interest and the decisions
- Reviews are referred to the level above the decision maker for his/her consideration

6. Directors

The Company's Act 2008, which is expected to come into effect in 2011, places a duty on a director to disclose any material information to the board regarding any business or contract the Company may be interested or involved in, and *not* to use his position to gain a personal advantage or to knowingly cause harm to the Company.

If a director (or his wife, family member, or other company which he controls) has a personal financial interest in any matter, business or contract in which the company is also involved or has an interest, he must disclose that interest in writing to his fellow directors.

If that interest relates to a matter to be considered at an upcoming board meeting, he must do the following:

- Disclose the interest and its general nature before the matter is considered at the meeting
- Disclose to the meeting any material information relating to the matter and known to the director
- Disclose any observations or insights relating to the matter if required to do so by the other directors
- Must leave the meeting immediately after making any disclosure and not take part in the consideration of the matter (For the purposes of maintaining the necessary quorum at that meeting, the absent director is still to be regarded as being present)
- Not execute any document on behalf of the company in relation to the matter

Annexure C: Moonlighting

Employees are not permitted to work on a part-time basis for any other employer or to offer their services in a consulting capacity, unless approval is obtained.

1. Approval

Where a staff member is involved in employment outside the Company the onus lies with the staff member to **inform** his/her manager, in writing, of such involvement and to **apply** for approval.

Application Form



employment_oustid
e_om_exemptio...

2. Exceptions to this rule

This rule will only be waived where the Company is not impacted by the following:

- The part-time employment is not in any way considered to be in competition to the Company
- The use of the skills involved is not considered to be prejudicial to our best interests
- Availability of the employee for overtime, shift work, etc
- Company time and resources are not used

Any application to waive this rule must be considered by the controlling senior Line Manager in consultation with the Risk Officer.

Annexure D: Gifts

Innocent business practices, like the giving and receiving of gifts could result in corrupt activities and may also be in contravention of the FAIS Conflicts of Interest Regulations. **The FAIS Conflicts of Interest Policy** deals with the exchanging of gifts (**an immaterial financial interest**) and limits the value of gifts exchanged in any calendar year.

Any person employed by an OMSA business unit may only exchange gifts which are allowed by **both** the Financial Crime Policy (Gifts) **and** the OMSA Rules regarding the exchange of "immaterial financial interests" in respect of FAIS. These rules limit the value of the "gift" to R100.00 or its equivalent at any single occasion or event with an overall limit of R1000.00 per annum. Please refer to the FAIS policy under the Code of Conduct on Groupnet which relates to gifts exchanged between Old Mutual, employees and our customers.

1. What this Policy covers

The Company recognises that we may receive, accept or give gifts to each other, and third parties eg. clients, suppliers, vendors, brokers, trustees. This business practice must be managed to avoid any perception of a conflict of interest or corruption.

This Policy provides guidelines for:

- The giving or receiving of gifts by employees and third parties
- What can be considered to be a gift
- Gifts which are allowed and those that are not
- When we need to seek approval before accepting gifts
- The recording of these activities

2. Allowed Gifts

The following are considered to be gifts which can be exchanged (given/received) between employees and third parties who are not employed by a Financial Services Provider (FSP).

Gifts under R1000 are allowed.

Examples

- An item (box of chocolates, bottle of wine, flowers)
- Goods (stationery, clothing, electronic equipment eg, cell phones, pc's)
- Services (spa and beauty treatments, including vouchers)
- A benefit (tickets to sporting and entertainment events, shows, meals, promotions)

Allowed gifts regardless of the monetary value.

NB: FAIS prohibits the gifts listed below if gifts are exchanged between employees of FSP's.

Examples

- Official COMPANY branded goods or items
- Official COMPANY sponsored functions, promotions or hospitality events
- Official donations made on behalf of the Company
- **Note:** This Policy does not apply to the exchanging of personal gifts between employees where the employee pays for the gift from their own funds for eg. Birthdays, weddings and other celebrations.

Rewards and incentives given to employees, are allowed, regardless of the monetary value. These need NOT be declared.

Examples

- Recognition awards such as gift vouchers, cash, holidays away
- Competitions such as Go For Leads, Disney awards, any lucky draws where employees can win prizes including weekends away, meals, etc.
- Where these gifts have been sponsored by Old Mutual or any Group Company
- Farewell gifts
- Old Mutual branded Promotional items

SARS considers the above gifts to amount to employee income and are therefore taxable

Business Units can choose one of the following tax treatments:

- Tax to be paid by employee: this reduces the value of the gift
- Tax to be paid by employer: the employee will receive the full value of the gift
- Your business unit HR manager must ensure that that these payments are reflected on the payroll.

3. Gifts not allowed

- Gifts exceeding R1000 are not allowed UNLESS prior approval by an Exco member has been obtained
- An employee's family may not give or receive gifts to third parties on the employee's behalf
- All travel for yourself or your family paid for by third parties
- Gifts that do not comply with the FAIS Conflict of Interest rules
- Gratuity (a sum of money given free of charge such as offering to pay a subscription or account)
- Gift vouchers, accommodation, conferences
- Money (cash, cheque)
- Donations (providing money, office equipment or other property to employees for charitable causes or out of generosity)
- The sponsorship of an employee (by contributing towards the cost of some project, course or activity) by companies who have a business relationship with Old Mutual

You may not accept or give more than one gift in respect of the same third party in any 3-month period. In addition, the value of gifts from the same third party may not exceed R1000 in the same calendar year.

4. Gifts to be declared

All gifts from, or given to, third parties must be declared irrespective of the value.

- Anything given or received over R1000 is not allowed. In exceptional cases for gifts over R1000 there must be written approval upfront and then it must be declared.

5. Gifts Register

- The Business Unit must appoint a responsible person to take ownership of the Gifts Register process which must be maintained and reviewed each quarter by a Risk, Compliance or Senior Manager
- The Head of GFS must be informed who they must liaise with at a Segment Level in order for a regular review of the Gifts Register to be conducted
- Employees must be able to access and view the Gifts Register
- All relevant details pertaining to the gift must be entered in the Register
- Disclosures must be filed in the Business Unit's Gifts Register and stored for 3 years before being deleted

6. Approval

Managers must:

- Proactively manage the receiving and giving of gifts
- Record, approve or decline gifts
- Provide guidance and advise on approvals
- When in doubt, seek advice from GFS

Annexure E: WhistleBlowing

This Policy guides you on how to raise concerns about possible unlawful and unethical conduct or breaches of company Policy in a safe way. It also provides information as to what should be reported and how you will be protected.

1. What this Policy does not cover

- Reports not made in accordance with the procedures in this Policy
- The Policy is not aimed at the reporting of employment grievances or general complaints. The Grievance Procedure is aimed at addressing issues where an employee is aggrieved or unhappy
- If your concern falls more properly within the Grievance Procedure, please act via the appropriate Human Resources (HR) channels

2. Concerns that can be raised and reported

- Criminal offences such as fraud, theft, corruption, money laundering and terrorism
- Any type of financial misconduct, including negligence
- Danger to the work environment or the health and safety of others
- Unfair discrimination
- Internal irregularities, including conduct that goes against any Company Policy or Procedure
- Concerns about wrongdoing may relate to any employee, including all levels of management, a colleague, an outsider, customer, broker, service provider, business partner or an ex-employee
- Concerns may also relate to past, present or future conduct
- Deliberate cover-up of any of the above
- Any other unlawful or unethical conduct relating to the workplace

If you are unsure as to whether an issue should be reported, ask yourself:

- Is the conduct legal?
- Is the conduct in line with the employee's contractual obligations to the Company?
- Is the conduct in line with our Policies and Procedures?
- Is the conduct in line with our values and Code of Ethics?
- Does the conduct feel right?
- Would you be happy if your manager, supervisor or colleagues were aware that you knew about the conduct and you did not report it?

Good Faith

- Concerns must be reported in good faith (good intentions).
- Those raised maliciously, for personal gain or reward may result in you not qualifying for protection under the Act or in terms of this Policy.
- Good faith reports that qualify for the protection of the Act are known as Protected Disclosures
- Knowingly making a false disclosure or making a disclosure with ulterior motives may also lead to disciplinary action being taken against that reporter.
- Proof of the allegation is not required, although this will be helpful

3. Your protection

The Company will take all reasonable steps to ensure that those who raise concerns in accordance with this Policy are protected from harassment, victimisation or other forms of unfair labour practices.

Only designated GFS staff members have access to the information supplied by you. Your information will be kept secure as all GFS staff have signed confidentiality agreements.