MSI Asia Pacific Speaking Up Policy

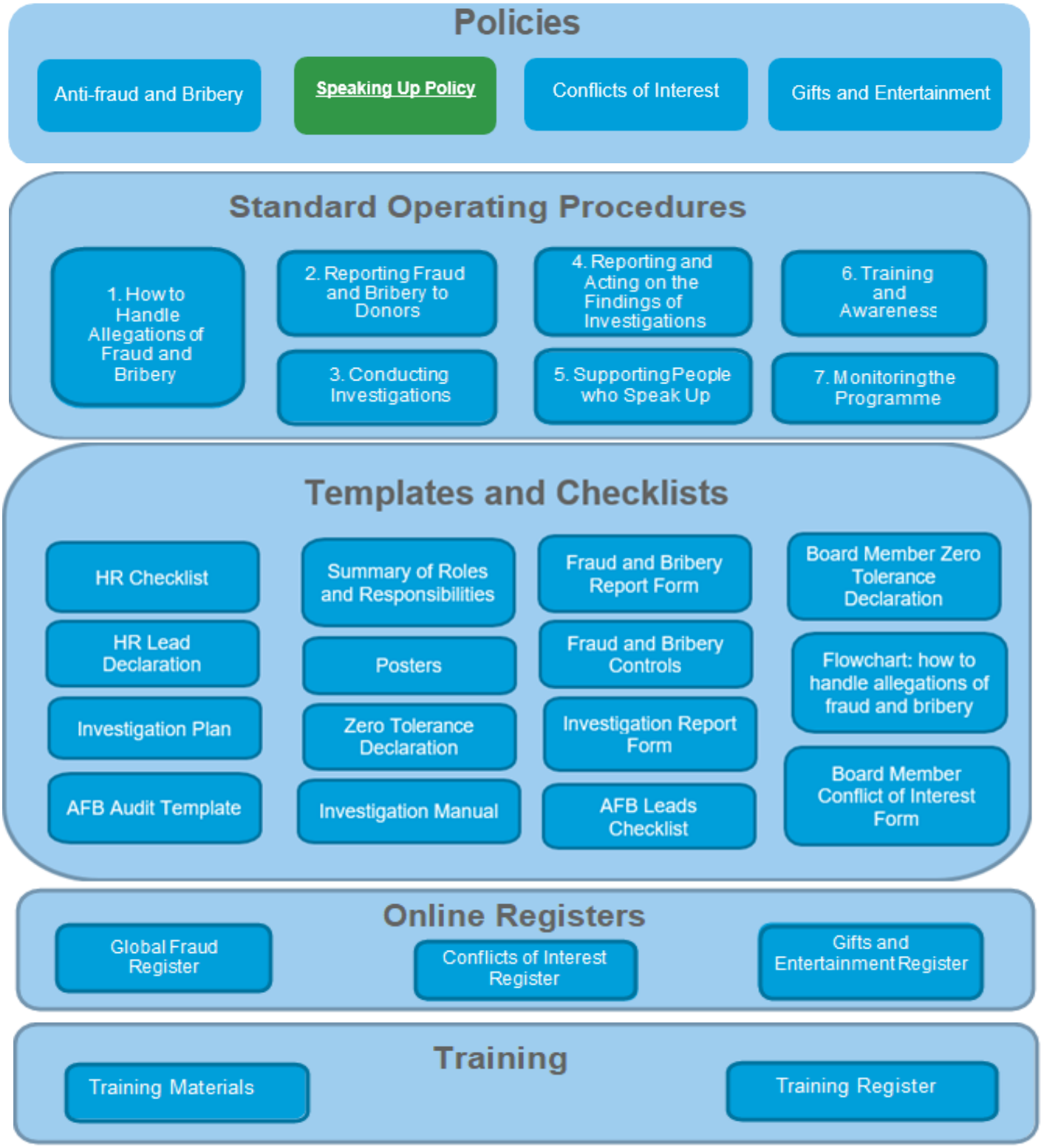
Policy Name:	**Speaking Up Policy**
Policy Number & Version:	**23.3**
Written By:	**MSI/MSIAP**
Date First Approved:	**N/A**
Last Amended By:	**MSIAP Finance Team**
Date Amendment Approved:	**June 2027 or when the global policy is updated by MSI – whichever is earlier**
Last Approved By:	**MSI Asia Pacific Board**
Date of Next Review:	
Policy Owner:	**MSIAP Finance Team**
Notes:	***This is a version of the Global MSI Policy which has been adapted for MSI Asia Pacific, in order to comply with region specific governance requirements.***

Contents

Policy Table: 3
Executive Summary 4
Introduction 4
1. Scope of the Policy 5
2. Why Speak Up? 5
3. Raising Awareness 5
4. What Should be Reported? 6
5. Protecting Those who Speak Up / Whistleblower protection 6
Support 6
Confidentiality 7
No reprisals 7
Anonymous allegations 7
Unfounded allegations 7
6. How to Raise Concerns 7
7. What Happens After You Raise Concerns? 8
How we respond 8
How we give you feedback 8
8. Monitoring and Review 9
Appendix 1 10
Safecall: Telephone Numbers by Country Programme and Support Office 10
Appendix 2 11

Fraud and Bribery Case Studies 11
Appendix 3 12
Safeguarding Case Studies 12
Other Case Studies 12

Policy Table:



Executive Summary

This Policy outlines how MSI People (as defined below) can report concerns in relation to **actual or potential wrongdoing or malpractice in MSI or its entities**.

If you have a concern, you may:

Use Speak Up Channels

Should you have a genuine concern about malpractice in the workplace (e.g. fraud, safeguarding, environmental issue), we require you to speak up using whichever one of the three below Speak Up Channels you feel most comfortable with:

Speak Up Channels:

1. Your line manager (or any manager if you believe that your line manager may be implicated)
2. Your Country Director
3. Safecall, the confidential, external and independent speaking up service consisting of:
    - a phone line (the numbers for which vary by Country Programme and are set out in the **Appendix 1** to this Standard Operating Procedure);
    - an email address: speakingup@safecall.co.uk; and
    - a website: www.safecall.co.uk/report.

Use Other Channels

Concerns may be raised in different ways than using the three Speak Up Channels and these concerns will be treated the same as if they were raised through a Speak Up Channel. Other channels include the Country Programme Contact Centre, where clients and external parties contact MSI through different touch points and report irregularities they may have encountered.

Introduction

This Policy is divided into eight sections and two Appendices:

1. Scope of the Policy
2. Why Speak Up
3. Raising Awareness
4. What Should be Reported?
5. Protecting Those who Speak Up
6. How to Raise Concerns
7. What Happens After You Raise Concerns?
8. Monitoring and Review

- **Appendix 1** contains the telephone numbers for Safecall in each Country Programme, the confidential, external and independent speaking up service.
- **Appendix 2 and 3** contain case-studies which illustrate the sorts of malpractice that may arise.

1. Scope of the Policy

1.1. This Policy is intended to enable those who become aware of actual or potential wrongdoing or malpractice in MSI or its entities to raise their concerns at the earliest opportunity so that they can be properly investigated. See Appendix 2 to this Policy for examples.

1.2. This Policy applies to all persons in the MSI Partnership, including all employees, contractors, MS Ladies, trainees, volunteers, sessional workers, and agency staff. All the persons to whom this Policy applies are collectively referred to as "**MSI People**".

1.3. This Policy may also apply to social franchisees, business partners (for example, suppliers) and to clients of MSI and its entities. Social franchises and other business partners (for example suppliers or consultants) are expected to adhere to the principles and values expressed in the Policy and subscribe to MSI's zero tolerance approach to.any incidence of malpractice in the workplace (e.g. safeguarding violations, fraud and bribery).

1.4. This Policy does not cover human resources issues, such as concerns about performance appraisals, promotion, contract renewal and salary. If you have these types of concerns, you should raise them under existing grievance procedures (in the case of employees) or under the contract which governs your relationship with MSI/its entities (in the case of contractors and franchisees), rather than under this Policy.

2. Why Speak Up?

2.1. MSI is committed to putting its clients first and continually delivering excellence. However, like all organisations, we face the risk of our activities going wrong from time to time and of unknowingly harbouring malpractice. As "One MSI", we need to work together to identify situations where this is happening and to rectify them as quickly as possible. Only by doing this can we improve.

2.2. MSI People are often the first to realise that there may be something going wrong. We therefore require you to speak up to us if you have genuine concerns about any behaviour in the workplace or how we are achieving our mission. By raising such concerns, you will be making a valuable contribution to our reputation and success. You will be helping us to serve our clients better and demonstrating the courage and integrity that is central to MSI's values.

2.3. If you are raising a concern, you should read this Policy. It explains:

- The type of concern that must be raised
- How to raise a concern
- How you will be protected against the risk of victimisation and harassment
- What will be done when you raise a concern

2.4. This Policy aims to:

- Encourage you to feel confident about raising concerns at the earliest opportunity
- Provide you with a clear procedure for raising your concerns
- Define a procedure to ensure that you receive a response to your concerns
- Reassure you that you will be protected from possible reprisals or victimisation where you have raised genuine concerns

3. Raising Awareness

3.1. This Policy is available on the Safeguarding and the AFB Programme pages on SharePoint.

3.2. All MSI staff are informed about this Policy and will either receive it directly or have access to it. Posters containing key information on how to raise concerns will be displayed throughout the offices of MSI and its entities. Client facing posters containing information on the specific mechanisms available to clients and community members for them to report cases of abuse and misconduct must be displayed throughout all service delivery points. Country programs are responsible for cascading MSI AFB policies and key donor fraud requirements to downstream partners at the project inception phase and to periodically monitor compliance throughout the project.

3.3. Training on the Policy is given to all MSI staff as part of the general training on MSI's Anti-Fraud and Bribery Programme and Safeguarding Programme. The Policy is also addressed in other MSI trainings. Senior management should also receive additional training on how to deal with concerns when they are raised, and how to protect the individuals who raise them.

4. What Should be Reported?

4.1. You must raise any concerns that you have about:

i. the conduct of colleagues, directors, trustees, business partners or others acting on behalf of MSI or its entities; or

ii. services provided by or to MSI or its entities, where the conduct or service provision:

- makes you feel uncomfortable in terms of known standards;
- is not in keeping with MSI or the relevant entity's policies and procedures;
- appears to be unethical, immoral or dangerous in any respect;
- appears to breach the law; and
- involves, or may involve:
    - sexual harassment, sexual misconduct, sexual abuse, or safeguarding issues;
    - terrorism or money laundering concerns;
    - harassment, bullying or discrimination;
    - breaches of privacy or confidentiality;
    - breaches of our Human Trafficking and Anti-Slavery Policy;
    - breaches of our Data Privacy policy;
    - fraud, bribery, deception or corruption;
    - neglect or abuse of clients;
    - unauthorised use of funds or other assets; or
    - damage to the environment.

This list is not exhaustive.

5. Protecting Those who Speak Up / Whistleblower protection

Support

5.1. MSI recognises that the decision to raise a concern can be a difficult one to make. If you have a genuine concern regarding the conduct of a colleague or MSI partner it is your duty to MSI/its entities, and all the clients who benefit from our mission, to speak up. You should have nothing to fear from reporting, as MSI must take active measures to support you throughout the process.

5.2. If you raise genuine concerns:

- you will be given full support from senior management;
- your concerns will always be taken seriously; and
- MSI will assign a contact person (known as the **Support Person**) to you and help you throughout any investigation.

Confidentiality

5.3. We hope that MSI People will feel able to voice their concerns openly under this Policy via the outlined reporting mechanisms. However, if you want to raise your concerns confidentially, MSI will make every effort to keep your identity secret. If it is necessary for anyone investigating your concern to know your identity, we will consult with you first whenever possible.

5.4. We will treat the identity of any victim(s), MSI People who speak up, and any person suspected of wrongdoing or malpractice as confidential, to the extent that we are able to do so. Information will be shared on a strictly need to know basis and never openly discussed. We may need to reveal individuals' identities in the course of a disciplinary process, employment tribunal or court proceedings or otherwise as required by law. Although it is not possible to give an absolute guarantee to the reporting person, or to anybody else who is involved in an investigation that confidentiality will be maintained, MSI will always make every effort to maintain confidentiality at all times.

No reprisals

5.5. MSI will not tolerate any harassment, victimisation, or other form of reprisal (including informal pressure), against any MSI People who raise concerns which they genuinely believe to be true and will take appropriate action to protect such MSI People. Any harassment, victimisation or other form of reprisal will be treated as a serious disciplinary offence and may result in dismissal. If you believe that you are being subjected to a detriment in the workplace as a result of raising concerns under this Policy, you should inform your Support Person immediately (see section 5.2 above).

Anonymous allegations

5.6. This Policy encourages you to put your name to the concerns you raise wherever possible. If you do not tell us who you are, it will be much more difficult for us to protect you or give you feedback.

5.7. However, concerns that are raised anonymously will not be ignored. We will consider whether we can investigate them considering:

- the seriousness of the concerns raised;
- whether the concerns appear credible; and
- whether we can sufficiently investigate the concerns based on the information provided, and if not, whether it is possible to confirm the concerns from other sources.

Unfounded allegations

5.8. If you raise a concern which you genuinely believe to be true, you will be supported under this Policy, even if the conclusion of the investigation is that you were mistaken.

5.9. If, however, you make a deliberately false or misleading allegation, MSI will consider taking appropriate disciplinary action against you.

6. How to Raise Concerns

6.1. If you have concerns, you must not attempt to investigate them yourself. You should raise concerns promptly with your line manager or, if you believe that your line manager may be involved in the issue that you are concerned about, another manager in your team. If you are not comfortable approaching either of those channels, you may raise concerns with either of the following:

- the Country Director (in the case of Country Programmes) or Team Director or Safeguarding Lead (in the case of Support Offices); or
- Safecall, the confidential, external and independent speaking up service which can be accessed by:

- a phone line (the numbers for which vary by Country Programme and are set out in **Appendix 1**)
- an e-mail address: speakingup@safecall.co.uk
- a website: www.safecall.co.uk/report; or

- You may use other channels, including the Country Programme Contact Centre or speaking to a manager who is not your line manager.

6.2. When raising concerns, you must give as much information as possible, such as relevant background information, names, dates, places and the reason for the concerns. You can raise concerns in writing, by telephone or in a face-to-face meeting. The earlier you speak up, the easier it will be for us to take effective action.

6.3. You are not expected to prove to us that your concerns are true. However, we do expect you to have reasonable grounds for your concerns, and to tell us why you think they may be true.

6.4. You may invite a colleague to be present for support during any meetings or interviews in connection with the concerns you have raised.

6.5. In most cases you should not find it necessary to alert anyone externally. Concerns raised under this Policy usually relate to the conduct of other MSI People, but they may sometimes relate to the actions of a third party. We encourage you to report such concerns internally first so that we can offer guidance and support.

6.6. In some circumstances it may be appropriate for you to report your concerns to an external body, such as a regulator. However, we strongly encourage you to seek advice before reporting a concern to anyone external to MSI, such as a donor (for donors please consult with the relevant Donor Lead). You may seek advice and report your concern using the confidential speaking up service (see section 6.1 above).

7. What Happens After You Raise Concerns?

How we respond

7.1. We will respond to your concerns as quickly as possible. Initial enquiries will be made to decide what next steps are appropriate. Concerns raised may be addressed in one or more of the following ways:

- investigated by the Country Programme or support office in question;
- investigated by Group Internal Audit;
- referred to the police (in cases involving Safeguarding this will only be done with consent of the victim);
- investigated by a relevant external body; or
- form the subject of an independent inquiry.

Some concerns may be resolved by agreed action without the need for an investigation. If urgent action is needed, this will be taken before any investigation is conducted.

How we give you feedback

7.2. After you have raised a concern, a Support Person will be assigned to you (see section 5.2 above). The person will, so far as possible:

- inform you about whether your concern will be investigated;

- give you an approximate time frame for dealing with the matter;
- inform you if your further assistance is required; and
- update you at the conclusion of the matter.

The amount of contact between you and those investigating your concerns will depend on the nature of the concerns and the clarity of your information. You may be asked to meet with those investigating so that they can be certain that they have fully understood your concerns.

7.3 Should an investigation be deemed appropriate, this will be conducted in accordance with MSI's commitment to carrying out thorough and objective investigations. More details of which can be found in MSI's Anti-Fraud and Bribery policy and AFB SOP3 Conducting Investigations.

8. Monitoring and Review

8.1. Various strategies will be used to monitor implementation of this Policy, including, but not limited to, the following:

- feedback on using the Policy will be sought from those who have raised concerns;
- statistics will be compiled on how the Policy is working in practice; and
- displaying Speak Up posters in accordance with this Policy will be monitored (including through the Anti-Fraud and Bribery Programme Audit – see Standard Operation Procedure 7: *Monitoring the Anti- Fraud and Bribery Programme*).

8.2. This Policy will be reviewed periodically by the Legal Safeguarding and Donor Compliance Team and by MSIAP as needed to reflect any changes to complaince requirements enacted by ACFID and DFAT.

Appendix 1

Safecall: Telephone Numbers by Country Programme and Support Office

NOTE: You will be charged to call the UK numbers below. However, you may ask to be called straight back. The free of charge numbers below may be called by you without charge to you. They are literally "free" as the charge will be passed to MSI.

UK Numbers	
Bangladesh	+44 191 5167756
Burkina Faso	+44 191 5167764
DRC	+44 191 5167764
Ethiopia	+44 191 5167764
Ghana	+44 191 5167764
Kenya	+44 191 5167764
Madagascar	+44 191 5167764
Malawi	+44 191 5167764
Mali	+44 191 5167764
Mongolia	+44 191 5167766
Myanmar	+44 191 5167761
Nepal	+44 191 5167775
Niger	+44 191 5167764
Nigeria	+44 191 5167764
Papua New Guinea	+44 191 5167764
Senegal	+44 191 5167764
Sierra Leone	+44 191 5167764
Tanzania	+44 191 5167764
Timor-Leste	+44 191 5167764
Uganda	+44 191 5167764
Yemen	+44 191 5167756
Zambia	+44 191 5167764
Zimbabwe	+44 191 5167764

Free of Charge Numbers	
Afghanistan	0790899499*
Australia	0011 800 72332255
Austria	00800 72332255
Belgium	00800 72332255
Bolivia	800 110328
Cambodia	1800 209761
China (China Telecom)	10800 4400682
China Unicom/Netcom	10800 7440605
India	000800 4401256
Mexico	01800 1231758
Pakistan	00800 900 44036
Romania	0372 741 942
South Africa	0 800 990 243
Sri Lanka (Colombo)	2423109
Sri Lanka (outside Colombo)	2423109
UK	0800 9151571
USA	1 866 901 3295
Vietnam (VNPT)	120 11157
Vietnam (Viettel)	122 80725

* (links to Safecall no +44 191 516 7787)

Appendix 2

Fraud and Bribery Case Studies

1. A member of staff in procurement noticed would-be suppliers of contraceptives handing unmarked envelopes of money to a colleague. The staff member reported the issue to their line manager who investigated and discovered that the colleague in question had been accepting bribes from would-be suppliers on a regular basis over the last two years. As a result of what the colleague had been doing, the Country Programme had not been sourcing its contraceptives from suppliers offering the most favourable terms and had been spending money on contraceptives that could have been used in other operational areas. The colleague accepting bribes was dismissed.

2. A member of the outreach team noticed another member, a nurse, falsifying figures to make it look like they had provided services to more women than was in fact the case. On the third occasion that they witnessed this, they decided to notify it to the Country Director. The concern was investigated and found to be true. The nurse was dismissed and MSI strengthened its data validation controls. MSI was able to inform the donors who were funding the outreach programme that it had identified several incidents of fraud and had acted quickly to deal with them, thereby winning the donors' respect and trust.

3. In one Country Programme, a member of the finance department had a long-standing grudge against a member of the audit team. They therefore pretended to their line manager that the member of the audit team had stolen contraceptives from the programme and sold them to a local hospital. On investigation, it was quickly discovered that there was no evidence to substantiate this concern and that it had been deliberately made up to cause trouble for the member of the audit team. The member of the finance department was dismissed.

4. One of the drivers in a Country Programme reported to Safecall that a fellow driver was using the programme's vehicles for personal purposes. The vehicle movements of the accused driver over the last few months and over the next month were carefully examined, and it was discovered that what the reporting driver had thought was a personal purpose was in fact a legitimate purpose that had been authorised by the Country Director. The Country Director responded to the reporting driver via Safecall and thanked the driver for bringing the concern to their attention and informed them that the concerns were investigated but found not be substantiated and the matter was dropped.

Appendix 3

Safeguarding Case Studies

5. A nurse works closely with a doctor. The doctor routinely tells the nurse that she is “looking good”, is “so pretty”, and “must have lots of boyfriends”. The doctor only makes these comments when the two are alone together. He frequently touches the nurse, including patting her on the back or thigh and telling her “job well done”. The doctor is widely respected as an intelligent and dedicated physician. He is always talking about the need to help women and so is seen as being supportive of women’s rights. The nurse feels very uncomfortable with this behaviour. She sends an email to the Country Director with her concerns. The Country Director requests HR to investigate the matter, and an official warning is given to the doctor, explaining that his conduct was inappropriate. The doctor made efforts to change his conduct and ensure he acted professionally. HR ensured the nurse felt comfortable and safe in her place of work and continued to monitor the doctor’s conduct.

6. A 32-year-old client visits MSI for assistance with long-acting contraception methods. A treating doctor closes the door behind the client as she enters the consultation room. After 10 minutes, the receptionist has a need to speak to the doctor and walks into the room after knocking. They see that the client is lying down on the table with her t-shirt and bra off and the Doctor is bent over her. The receptionist is very apologetic as the doctor should not let her enter the room during a consultation. As the client leaves, she pays for an IUD insertion. The receptionist is further confused as this service does not require the client to remove her top or bra. The receptionist sends an email to Safecall. The Safecall report is forwarded to the Country Director who launches an investigation. The doctor is suspended, and the investigation reveals a pattern of inappropriate behaviours. The doctor is dismissed, and the national medical board is informed.

7. A support office team member experiences lewd comments and jokes from a senior female manager. When challenged by the team member, the senior manager responds: ‘*It was just a joke*’. The manager acknowledges that the team member was uncomfortable and stops making such comments towards them. However, she continues to make similar lewd jokes and comments towards other team members. This is observed by the team member and reported via email to the HR Manager. HR investigate the matter and hold a meeting with the senior manager on the use of inappropriate language in the work place. They refer the manager to the Sexual Harassment Policy and remind her that harassment is judged based on the recipient, and that she must consider the view points of team members who may not consider such jokes appropriate. A formal warning is given to the manager, with a record kept on her file.

Other Case Studies

8. A doctor in one of the Country Programmes saw repeated instances of client safety procedures being ignored by members of staff in a clinic. The doctor was anxious that their line manager might take these concerns as personal criticism, so he used Safecall to raise them. At MSI’s request, the Country Director of the programme carried out an investigation into the concerns, which resulted in the doctor’s line manager and one nurse being taken through a disciplinary process and a change in client safety protocols being implemented.

9. A partner NGO routinely changes their method for payment. On occasion, they have been insistent on being paid in cash and at times they have been insistent on being paid in various foreign bank accounts, despite holding offices locally. The finance assistant raised the concern with their line manager, the Finance Director. A decision was made to stop using this supplier and to report the organisation in line

with anti-terrorism legislation requirements.

10. MSI is partnering with a local Ministry of Health (MOH) as part of PSS. An MSI nurse overhears an MOH employee taking a personal call during their lunch break in which they discuss clients who attended appointments that day by their name. The MSI nurse is very concerned by this breach of client confidentiality and data privacy and informs their Country Director. The Country Director speaks to the MOH Manager and the employee is suspended and receives immediate training on data privacy