BEYOND

Surpassing Boundaries

Security Protocols

Safe communication & living protocols for Beyond Workers

(Confidential)

PLEASE LEAVE THIS DOCUMENT AND ALL TRAINING MATERIALS IN A SECURED LOCATION.

Do not under any circumstances take these materials on your trip overseas or when you travel.

beyond@oncrest.ca

Table of Contents

BEYOND Security and RAN Rational

Risk is necessary:

We are only at TEMPORAL risk when we do things for God. We are at ETERNAL risk only when we do nothing for God. Therefore, risk is necessary. In fact, persecution for Christ's name sake should be considered normal to the Christian life (1 Pet. 2:20, 21, Phil. 2:3-8, John 15:20 etc.). But let's make that risk for the right reason and also be careful not to be careless. Furthermore, we exercise wisdom and security for the sake of workers & their families in secure regions, other associated workers and other believers in these secure regions.

Security is necessary:

Many countries or regions are considered **Restricted Access Nations (RAN)** or Secure Regions. This means that it may be illegal to enter as a "missionary", illegal to "proselytize" for conversion, illegal to distribute "Christian" literature, or illegal to meet as foreign Christian believers. This can be punishable by expulsion, imprisonment or even death. In other cases, it may not be illegal or punishable in the government's eyes, but the local population or society may take extreme action against anyone displaying these behaviors. Furthermore, scrutinized unsecured communication, phone tapping and paid informants are potential realities for a RAN worker. Thus, for the sake of long term effectiveness and security of Global Workers & their families and local believers, we practice tight security protocols in RAN's.

BEYOND Security Regions and Levels

BEYOND recognizes that each region and country of the world carries their own unique security levels, risks and challenges. Therefore, BEYOND leaves discretion and determining security levels up to each Global Worker and / or team in consultation with the BEYOND Oversight Team. Until this is fully determined by each Global Worker and / or team, tighter security levels should be followed. This handbook outlines a relatively tight security level while leaving room for future *loosening* or *relaxing* of these protocols once Global Workers / Teams and the BEYOND Oversight Team have determined that this would be acceptable.

Universal Declaration of Human Rights (UDHR Ar. 18)

"Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief, and freedom, either alone or in community with others and in public or private, to manifest his religion or belief in teaching, practice, worship and observance."

All nations have signed this with the exception of Saudi Arabia. However, few RA Nations honor it.

BEYOND Security Protocols for Global Workers

Public Profile

This is your profile that is determined by your Role and Identity. A Global Worker's role and identity must be authentic, viable, real, integrous and fit with the context each Global Worker is working in. A Global Worker's public profile will be open to public scrutiny and the following protocols will keep one's profile secure. Most of one's communication should be done using this public profile, using security conscience vocabulary and protocols.

Electronic Communication

1. Email

   An email address, other than gmail your Secure Profile email address, should be used. Particularly, we recommend Apple mail, outlook.com or hotmail.com or the like. Avoid the use of any email address that could contain a missionary, church or christian name. This email address should be used regularly and anyone using this email address should understand security protocols for communicating to this email address.

2. Social Media

   A public social media profile provides an excellent way to show authenticity when under scrutiny.

   A. Establish this profile before leaving for field of posting. Populate that profile with relevant, non-missionary information or pictures.

   B. Only "friend" those who can be trusted to communicate securely with you or will not undermine your role and identity or profile.

   C. It can be a separate profile from your more secure social media profile if you choose to have two social media profiles.

3. Skype etc.

   A. A Skype (or similar) account should be set up which you would use to connect with friends and family back home and in country.

   B. Skyping someone at a Skype user name that could cause suspicion should be avoided.

   C. Communication with Skype can be considered secure, but this is not guaranteed. One should consider all Skype communication monitored. Therefore, security conscious vocabulary & protocols should be used.

4. Internet

   A. Use "Bing" or a similar search engine as a preferred search engine (due to security concerns) rather than "google".

   B. Regular internet surfing and usage done properly will reinforce your identity.

C. Remember that any web site, search or app that you use can be monitored. Therefore, security conscious practices & protocols when using these forms of media should be followed carefully.

Telephone Communication

1. All telephone communication should be considered "insecure" and is most likely monitored.
2. One should consider all telephone communication monitored or tapped. Therefore, security conscious vocabulary should be used.
3. Use of mutually understood acronyms or "coded" words should be used if discussing secure information, names, places etc.

General Communication Protocol

1. Do not name any fellow Global Workers or local believers by name. Either use mutually accepted pseudo names or initials only.
2. Do not name any countries, cities, neighborhoods, locations directly. Use generalities.
3. Do not mention anything to do with "mission", "church" or "Christian" work publically. Use "code" words where necessary.
4. Do not post pictures linked to "Christian" or "Missionary" work, locations or Secure Profiles.
5. Do not comment on political, social or religious issues within your country / area.
6. Avoid references to Islam, Mohammed, the Quran, 9/11, terrorism, or any other potentially political or religiously inflammatory issues.
7. Avoid reference to any "specific" churches or denominations or missions organizations in Canada or elsewhere.

Secure Profile

When communicating between BEYOND team members, BEYOND Oversight Team or other designated persons (i.e. Newsletter Liaison) regarding secure information, the following protocols should be followed:

Secure Private Profile process:

1. Connect to Private Connection:
   A. Log on Private Tunnel (https://www.privatetunnel.com)
   B. Use Internet Explorer, Safari or other "more secure" browser.
   C. Set In-private browsing on browser. *A safe practice is to always carry on "private" browsing with someone you are accountable to.*
2. Connect to Secure Silo:
   A. Log on to Office 365 (https://login.microsoftonline.com/).

B. Use your assigned globalexperience.info email and password to log on to GlobalExperience Secure Silo.

C. Conduct any work necessary on the Secure Silo (e.g. Email, read documents).

3. Exit Secure Silo:
   A. When finished with your work on the GlobalExperience Secure Silo, LOG OFF.
   B. Take off In-Private browsing on your web browser.
4. Conduct legitimate activity:
   A. Do some Canadian or US related online activity (e.g. banking for a brief time or something similar).
5. Exit Private Connection
   A. Log off private tunnel.

Living Security

Rules for a Secure Home

1. Guard info about yourself and what you do. Keep family info private (need to know).
2. Put secure locks (and possibly gates or bars) on all doors and windows
3. Install a "peephole" in your door
4. Be aware of and take note of any bags that come through your door.
5. Do not open the door to strangers (esp. kids are not to open the door)
6. Do not talk about where we keep our money, computer, or what our escape plans are or how we are protecting our home and ourselves.
7. Memorize key phone numbers.
8. Always tell each other where we are going and when we expect to arrive/return.
9. Have a "Safe Room" at your home.

Rules for a Secure Neighborhood

1. Recognize and Report unusual or suspicious behavior (kids too).
2. Keep a low profile by the way you conduct yourself and dress.
3. When walking, keep your handbag on the side away from the road, and if possible walk next to a wall or building
4. Make friends with your neighbors and local shopkeepers and establish good relationships with them. Are they willing to help you/inform you/ teach you what to do?
5. Listen to the advice of your neighbors.
6. Be alert and aware of what is going on around your neighborhood

7. Be suspicious of unusual people or activities in your area.
8. Refuse to meet new people (strangers) at a time and place of their choosing (many kidnappings happen that way).
9. If you think you are being followed, go to a pre-selected area. Do not lead the person to your home.

Rules for Secure Kids

1. Kids shouldn't accept food or drinks from anyone without mom/dad's permission.
2. Do not leave your children unattended.
3. Don't go anywhere with another adult unless mom or dad has directly told you that it is alright.
4. Teach your kids that no one touches them in their private areas – they MUST tell someone if it happens.
5. Come up with a universal CODE WORD if a co-worker has to come to rescue children in the home if something has happened to their parents (or has kept them away).
6. Have a child care plan if something happens to the parents (who will the kids go to; who will come to get the kids).
7. Pick a "safe haven" to meet at if children get lost (ie: near the cashiers at the front of the store). OR go to a mother with children to ask for help.

Rules for a Secure Team

1. Have an evacuation plan from your city.
2. Have an early warning system between team members and local partners.
3. Team leaders should make Canadian leadership aware of "threats" (i.e. Religious radicals come to the village with their loud speakers to speak out against the Christians being there).

General Rules for Secure transportation

1. Always lock all the doors, including when you are inside the vehicle
2. Always ensure the trunk is locked
3. When walking to your car, have your keys ready in your hand so you can enter as quickly as possible, also check for suspicious wires or unusual packaging or "garbage" lying around the vehicle
4. Put packages in the trunk - out of sight
5. Always keep your car half full of fuel
6. Keep a safe distance between you and the car in front
7. Regularly check your rearview mirror to see if you are being followed
8. If possible, park in well-lit areas

9. If you are making a pit-stop, never leave the keys in the ignition even if there are others in the vehicle
10. If you unexpectedly drive into an area with a riot in progress, keep the vehicle moving and quickly check for the shortest escape route. You want to get out of this situation as quick as possible. If necessary drive over curbs, sidewalks, flowers, etc. Keep your speed up so that you don't get trapped in the middle of things and lose momentum. Find the quickest way out and get there. If you don't give a chance for the rioters to think about you except to stay out of your way you should be able to get out. Do not ram into pedestrians or you will have the crowd's wrath on you instead of the reason they are rioting.
11. Always be aware of who is around you when on public transportation. If you feel that you are being followed, go immediately to a public, safe area and make contact as soon as possible with someone from your team or a trusted individual.

Evacuation Planning

There are a number or sources that may indicate that an evacuation is necessary. They are:

1. Canadian High Commission or US Embassy Recommendations
2. Input from other individuals and companies
3. Personal observations and feeling of team
4. Children's Schools
5. Trusted National Friends
6. Team consensus for level of alert
7. Company Directive

Determine who is the primary person on your team designated to communicate with authorities, media, home team and whoever.

There are a number of levels of alert:

1. Code **Blue** – Low

   Local riots/demonstrations not directed at team, international conflict or war in region
2. Code **Yellow** - Moderate

   Local attack on westerners, personal threats
3. Code **Red** – High

   Imminent danger, war in country, strong recommendation that foreigners depart

Who evacuates first?

1. Children & their mothers
2. Whole families with children
3. Fathers (whose children & wives have preceded)
4. Families without children

Code Level Responses:

1. **Code Blue**
   - A. Take caution, avoid troubled areas
   - B. Avoid political discussions
   - C. Vary local travel and habitual patterns
   - D. Confirm that personal documents are current and secure
   - E. Carry photocopies of documents
   - F. Confirm that any 'sensitive' material is secure
   - G. Secure food supply for one month
2. **Code Yellow**
   - A. Stay at home
   - B. Make plans with children's schools
   - C. Make/Check travel plans
   - D. Two suitcases packed (one small one with travel docs & important basics)
   - E. Daily contact with other Team Members
   - F. Check information & news regularly (with other orgs and individuals)
   - G. Begin Security Process (for personnel & possessions)
   - H. Evaluate Code Red Preparations (for possible First Stage Evacuations)
3. **Code Red**
   - A. Prepare Real & Personal Property
     - Household perishables & vehicles to friends
     - Home locked, keys to friends with instructions
   - B. Review Check Lists
     - To Do – One hour notice
     - To Do – 24 hour notice
     - To Take – medications, clothing, documents, equipment
   - C. Prepare Funding (should already be on check lists)
     - Cash, (appropriate currencies)
     - Bank & Credit Cards
   - D. On Instruction – Move to Staging Point ASAP
     - If Regional by land – convoy if at all possible
     - If International by air – nearest port or airport

BEYOND Security Protocols for Partners

Guidelines

Guidelines for communicating with Christian workers / Global Workers in Restricted Access Nations (RAN). Revised – Sept 2014

Introduction

Today's world has a drastically changing socio-political landscape. New measures and safeguards are needed in global communications. Unsecured email; tapped phone lines; and paid informants all present potential security breaches to our Christian workers in resistant contexts. The fallout from a careless phone conversation or church website with too much information can have life threatening consequences for our workers and national Christians.

The following guidelines simply serve to provide a framework for meaningful interaction between Christian workers in RAN contexts and support personnel from the Mission Agency or Home Church office (pastors, administrators, mission's leaders etc.). As senders the last thing we want to do is compromise anyone's safety.

Communication

Email and internet use has exploded in the past five years. We can literally communicate with anybody anywhere as long as we have access to a modem and a computer. However, not all email is secure. In fact, most is not. Sent emails are stored on servers around the world as they travel through cyberspace and can be easily read by people with access to those servers.

Chief rules to follow:

"The Field Staffer / Global Worker is the person at risk. Therefore, he/she/they MUST be allowed to determine their own level of risk, and we, the supporting structure, MUST honor their requests in this regard for their safety sake"

Here are a few basic guidelines for general communication with workers that includes email, fax, regular mail and packages:

1. Expect your letters and/or packages to be opened by government officials responsible for censoring incoming/outgoing communications. Not all mail is read, but keep this in mind as you write.
2. Never use Church or organizational letterhead or envelopes. Use blank paper and plain envelopes.
3. Do not ask the worker to comment on political, social or religious issues within the country or the RAN world in general.
4. Avoid references to September 11, terrorism or other potentially inflammatory issues.

5. Do not ask the Christian worker to divulge the names, locations or details of other Christian workers, or national believers.
6. References to Islam, the Quran or Mohammed, inflammatory or otherwise, should be avoided.
7. Avoid mentioning specific churches in Canada or in the worker's adopted nation.
8. Avoid using 'titles' such as 'Rev.' Use personal names only.
9. Avoid using an email address with a church or mission agency name. For example dsmith@bethelchurch.org
10. If you are writing and mailing letters, consider numbering them. Sometimes they get lost en route.
11. Never send Bibles into the RAN world without the permission of, and specific preparation in consultation with the receiving party
12. If you support or are in communication with a worker in a resistant context, consider paying for a secure email account for them. Go to a secure service provider such as www.generalmail.com for purchasing secure email services.
13. Get knowledgeable advice concerning Encryption. Ask your supported worker as to his/her preference in using encrypted e-correspondence.
14. If you are sending packages to workers, DO NOT include books, magazines, articles, CDs or tapes about evangelism, Islam or missions unless specifically asked by the field worker to do so. Packages are often opened and inspected by customs officials.
15. It is perfectly acceptable to send Christmas and Easter cards celebrating 'western' religious holidays.
16. The bottom line is to use common sense and not put our Christian workers in any compromising situations.

Avoiding 'Christianese'

As evangelicals we are notorious for the 'Christianese" we speak. This can be especially problematic in our communications with workers. Certain words raise suspicion among officials in other countries. Some potentially alarming words can be substituted with other 'code' words. Examples:

WORDS TO AVOID:	**ALTERNATE WORDS:**
Missionary	*Member or Worker*
Muslim or Hindu etc.	*M or H or Neighbor or Cousin*
Christian/Believers	*Family*
Church	*House*

Evangelism	*Sharing*
Missions	*Work*
Born Again/Salvation	*Change*

1. Be careful not to write veiled messages. These can arouse suspicion from those who will be observing the Christian workers.
2. If your church is actively involved in the RAN world, the worker you support may have 'code' names for these countries. Please honor their desire to use these terms.
3. Some workers in very restricted areas may also desire to use a 'pseudonym' when speaking at home. Please honor this request. Feel free to discuss this with the worker to understand his/her situation.

Promotions

Not only do we need to be "wise as serpents and harmless as doves" in our communications with workers, we also need to be cautious in how we promote them at home. The following guidelines can apply to websites, bulletin boards, prayer inserts etc.

Chief Rule:

Again, the field staffer MUST be allowed to set the bar for this in your church. Please respect their requests for specifics, but use the following as a general rule of practice.

1. A good rule of thumb to adopt is ***No names, No faces, No places combined***. Pictures of Christian workers or national workers should not be posted or printed publicly in connection with their 'last name' and or 'specific location'.
2. Specific locations should be avoided. General geographic areas/regions can be used instead (i.e. North Africa, Middle East, South East Asia).
3. It is not advisable to use complete or actual names. First names only or even initials are preferred.
4. Get permission from workers in RAN locations before distributing their newsletters, prayer updates or email addresses.
5. Use wisdom when profiling the RAN world. Avoid inflammatory or biased viewpoints and information.
6. Use wisdom when advertising mission's speakers from the RAN world. There are many active Islamic groups in North America who track the work of Protestant missions groups.

Security Protocols for Travel to RA Nations

In the event that you as a partner travel to visit a Global Worker / Partner in their RAN place of deployment, certain protocols should be followed. These protocols are called Safe Travel Protocols.

Communications Basics

Spend some time before you go to develop answers to these questions:

1. Who are you and what group are you with? (Public information about your group.)
2. What are you going to do?
3. Why would you come to work in this country?
4. Who sent you? Who supports you?
5. With whom are you working?

Work with partners in the overseas location to make sure there is a clear "**Simple Truth Statement**" (STS) that can be used. In answering the questions above, the STS should be developed and used.

Church members, family and friends in United States should know and understand your STS, and use it as the basis to share information with others and with the media.

There also are some harder questions that need to be addressed BEFORE they are ever needed:

1. Are you a missionary or are you working with missionaries? Why is your church or family in the United States identifying you as a missionary?
2. Are you connected to a missions organization?
3. Are you here to convert our people to Christ?

In developing answers to these questions, remember that you can speak truth without sharing all you know. Remember your STS and stay within the four corners of the box.

Safe Travel Solutions Basics

1. Someone in the United States needs to be designated as the spokesperson for your team. Friends and family should refer all inquiries from the media to this person.
2. All team members should know this person and his/her role. Make appropriate contact information available to all who need it.
3. All media inquiries should be referred to the spokesperson unless the decision is made to handle a particular situation differently.
4. If possible, the spokesperson should remain in that role for the duration of the crisis. If at all possible, the spokesperson should not be the senior leader of the sending entity (church or mission group).

5. The spokesperson and leadership members should discuss in advance how approvals of statements should work. Who needs to be involved? Who has the authority to make the decision about the information to be released?
6. The company or organization you are partnering with on the field can assist in shaping messages and working with the media. When a situation occurs, the first contact (before a response is issued) should be with the partnering organization.

Security Protocols for working with Media

Who is your audience?

The reporter is not your entire audience. You are speaking to the whole world, including those in the country where the team is working, government officials in their country and the United States, perpetrators, family, church family and the general public. The reporter is the conduit to all of these audiences.

Responding to Inquiries from the Media

Be friendly and courteous but don't make a commitment to participate in an interview or answer questions until you know the nature of the call.

Consider if the team and the work would benefit or be harmed by participating in the interview.

(In a crisis that is public in nature, there must be a response to the media. However, the response that is made should not be decided on the basis of the first inquiry.)

Ask questions:

1. Who is calling?
2. What kind of story are you working on?
3. What questions do you have?
4. Who else have you talked to?
5. Others (supporters and non-supporters of your cause) will be speaking.
6. What is your deadline?

In a crisis, a statement should be issued as soon as is feasible, but it is important to make sure that decisions and approvals have been made about the information to be released. The information must be consistent. How can I best reach you?

Consider if others need to hear information directly from the company before it is released through the media (i.e., personnel, family, company).

Crisis Message Development Goals

1. Get messages to the audiences.
2. Determine three to four key points that need to be shared.
3. Make sure messages have been shaped and approved by those in leadership who are dealing with the crisis. Also, coordinate messages with the partnering organization.

4. Mitigate damage.
5. Be the best source of the correct information.
6. Consider how to protect voice, presence and life.
7. Be consistent
8. Bridge (reinforce) your message(s) with each answer.
9. Avoid answering with "No Comment."
10. Find another way to (not) answer the question.
11. "No comment" indicates avoidance or guilt.
12. Avoid "off the record" comments. There is really no such thing; the reporter will find a way to get the basic information into the story.
13. Remember: Reporters get to ask the questions, but we get to choose which answers to give!

Ways to Respond to Questions

1. Give direct and immediate answers.
    A. - These are responses to questions that are anticipated and for which answers are prepared.
    B. This is your opportunity to get the correct facts and your messages to your audiences.
2. Answers should be short and to the point (think 10-12 second sound bites).
    A. Don't give more information than was requested, but do bridge to your message. Don't ramble.
    B. If you need to think through your answer or buy a little time:
        i. Ask the reporter to repeat the question.
        ii. Repeat the question yourself. (And if it was negative, rephrase it. If it was too broad, you can narrow it or if it was too narrow, you can broaden it.)
        iii. Share your thought process with your audience. (Example: "That is an interesting question, and I need to think for a minute about how to help your listeners understand the situation.")

Questions you do not have to answer

(But be sure to explain why you are not answering them)

1. Personal questions
2. Hypothetical (What would your company do IF this happened?)
3. Questions involving legalities or negotiations
4. Third-party questions (You should answer only for your company.)
5. It is fine to say, "I don't know." (bridge to your message "What I do know is... ")
6. Avoid the "No comment" response.

BEYOND Security Protocols for Agency Staff

Guidelines

Guidelines for communicating with Christian workers / Global Workers in Restricted Access Nations (RAN). Revised – Sept 2014

Introduction

Today's world has a drastically changing socio-political landscape. New measures and safeguards are needed in global communications. Unsecured email tapped phone lines and paid informants all present potential security breaches to our Christian workers in resistant contexts. The fallout from a careless phone conversation or church website with too much information can have life threatening consequences for our workers and national Christians.

The following guidelines simply serve to provide a framework for meaningful interaction between Christian workers in RAN contexts and support personnel from the sending church (pastors, mission's leaders etc). As senders the last thing we want to do is compromise anyone's safety. This document will focus on two key components; communication and promotions.

Communication

Email and internet use has exploded in the past five years. We can literally communicate with anybody anywhere as long as we have access to a modem and a computer. However, not all email is secure. In fact, most is not. Sent emails are stored on servers around the world as they travel through cyberspace and can be easily read by people with access to those servers.

Chief rule to follow:

"The Field Staffer / Global Worker is the person at risk. Therefore, he/she/they MUST be allowed to determine their own level of risk, and we, the Supporting Structure, MUST honor their requests in this regard for their safety sake"

Here are a few basic guidelines for general communication with workers that includes email, fax, regular mail and packages:

1. Secure or "security sensitive" communication should always be done through the BEYOND communications coordinator who has direct access to communicating through the Global Workers secure email address. Forward email / documents to be sent to them first and they will forward them accordingly.
2. Expect your letters and/or packages to be opened by government officials responsible for censoring incoming/outgoing communications. Not all mail is read, but keep this in mind as you write.
3. Never use Church or organizational letterhead or envelopes. Use blank paper and plain envelopes.

4. Do not ask the worker to comment on political, social or religious issues within the country or the RAN world in general.
5. Avoid references to September 11, terrorism or other potentially inflammatory issues.
6. Do not ask the Christian worker to divulge the names, locations or details of other Christian workers, or national believers.
7. References to Islam, the Quran or Mohammed, inflammatory or otherwise, should be avoided.
8. Avoid mentioning specific churches in Canada or in the worker's adopted nation.
9. Avoid using 'titles' such as 'Rev.' Use personal names only.
10. Avoid using an email address with a church or mission agency name. For example dsmith@bethelchurch.org
11. If you are writing and mailing letters, consider numbering them. Sometimes they get lost en route.
12. Never send Bibles into the RAN world without the permission of, and specific preparation in consultation with the receiving party
13. Get knowledgeable advice concerning Encryption. Ask your supported worker as to his/her preference in using encrypted e-correspondence.
14. If you are sending packages to workers, DO NOT include books, magazines, articles, CDs or tapes about evangelism, Islam or missions unless specifically asked by the field worker to do so. Packages are often opened and inspected by customs officials.
15. It is perfectly acceptable to send Christmas and Easter cards celebrating 'western' religious holidays.
16. The bottom line is to use common sense and not put our Christian workers in any compromising situations.
17. When a phone call or other communication is received regarding any "potential" missionary work or Global Workers, follow standard agency security protocol and answer using the protocols printed separately and forward to BEYOND staff immediately.

Avoiding 'Christianese'

As evangelicals we are notorious for the 'Christianese" we speak. This can be especially problematic in our communications with workers. Certain words raise suspicion among officials in other countries. Some potentially alarming words can be substituted with other 'code' words. Examples:

WORDS TO AVOID:	ALTERNATE WORDS:
Missionary	*Member or Worker*
Muslim or Hindu etc.	*M or H or neighbor or cousin*
Christian/Believers	*Family*
Church	*House*
Evangelism	*Sharing*
Missions	*Work*
Born Again/Salvation	*Change*

1. Be careful not to write veiled messages. These can arouse suspicion from those who will be observing the Christian workers.
2. If your church is actively involved in the RAN world, the worker you support may have 'code' names for these countries. Please honor their desire to use these terms.
3. Some workers in very restricted areas may also desire to use a 'pseudonym' when speaking at home. Please honor this request. Feel free to discuss this with the worker to understand his/her situation.

Promotions

Not only do we need to be "wise as serpents and harmless as doves" in our communications with workers, we also need to be cautious in how we promote them at home. The following guidelines can apply to websites, bulletin boards, prayer inserts etc.

Chief Rule:

Again, the field staffer / Global Worker MUST be allowed to set the bar for this in your church. Please respect their requests for specifics, but use the following as a general rule of practice.

1. A good rule of thumb to adopt is ***No names, No faces, No places combined***. Pictures of Christian workers or national workers should not be posted or printed publicly in connection with their 'last name' and or 'specific location'.
2. Specific locations should be avoided. General geographic areas/regions can be used instead (i.e. North Africa, Middle East, South East Asia).
3. It is not advisable to use complete or actual names. Pseudo names or even initials are preferred.
4. Get permission from workers in RAN locations before distributing their newsletters, prayer updates, blog posts or email addresses.

5. Use wisdom when profiling the RAN world. Avoid inflammatory or biased viewpoints and information.
6. Use wisdom when advertising mission's speakers from the RAN world. There are many active Islamic groups in North America who track the work of Protestant missions groups.

Security Protocols for working with Media

Who is your audience?

The reporter is not your entire audience. You are speaking to the whole world, including those in the country where the team is working, government officials in their country and the United States, perpetrators, family, church family and the general public. The reporter is the conduit to all of these audiences.

Responding to Inquiries from the Media

Be friendly and courteous but don't make a commitment to participate in an interview or answer questions until you know the nature of the call.

Consider if the team and the work would benefit or be harmed by participating in the interview.

(In a crisis that is public in nature, there must be a response to the media. However, the response that is made should not be decided on the basis of the first inquiry.)

Ask questions:

1. Who is calling?
2. What kind of story are you working on?
3. What questions do you have?
4. Who else have you talked to?
5. Others (supporters and non-supporters of your cause) will be speaking.
6. What is your deadline?

In a crisis, a statement should be issued as soon as is feasible, but it is important to make sure that decisions and approvals have been made about the information to be released. The information must be consistent. How can I best reach you?

Consider if others need to hear information directly from the company before it is released through the media (i.e., personnel, family, and company).

Crisis Message Development Goals

1. Get messages to the audiences.
2. Determine three to four key points that need to be shared.
3. Make sure messages have been shaped and approved by those in leadership who are dealing with the crisis. Also, coordinate messages with the partnering organization.

4. Mitigate damage.
5. Be the best source of the correct information.
6. Consider how to protect voice, presence and life.
7. Be consistent
8. Bridge (reinforce) your message(s) with each answer.
9. Avoid answering with "No Comment."
10. Find another way to (not) answer the question.
11. "No comment" indicates avoidance or guilt.
12. Avoid "off the record" comments.
13. There is really no such thing; the reporter will find a way to get the basic information into the story.
14. Remember: Reporters get to ask the questions, but we get to choose which answers to give!

Ways to Respond to Questions

1. Give direct and immediate answers.
    A. - These are responses to questions that are anticipated and for which answers are prepared.
    B. This is your opportunity to get the correct facts and your messages to your audiences.
2. Answers should be short and to the point (think 10-12 second sound bites).
    A. Don't give more information than was requested, but do bridge to your message. Don't ramble.
    B. If you need to think through your answer or buy a little time:
        i. Ask the reporter to repeat the question.
        ii. Repeat the question yourself. (And if it was negative, rephrase it. If it was too broad, you can narrow it or if it was too narrow, you can broaden it.)
        iii. Share your thought process with your audience. (Example: "That is an interesting question, and I need to think for a minute about how to help your listeners understand the situation.")

Questions you do not have to answer

(But be sure to explain why you are not answering them)

1. Personal questions
2. Hypothetical (What would your company do IF this happened?)
3. Questions involving legalities or negotiations
4. Third-party questions (You should answer only for your company.)

5. It is fine to say, "I don't know." (But bridge to your message … "What I do know is …")
6. Avoid the "No comment" response.

Final Thoughts

These guidelines and suggestions are in no way meant to discourage you from communicating with workers. It just takes a higher degree of precaution than in other parts of the world.

Our workers love to hear from home. Encouragement can come in many different ways.

Remember, it takes a core team of support people (Senders) around every Global Worker / Christian worker. The responsibility of sending can involve children, youth, families and seniors.