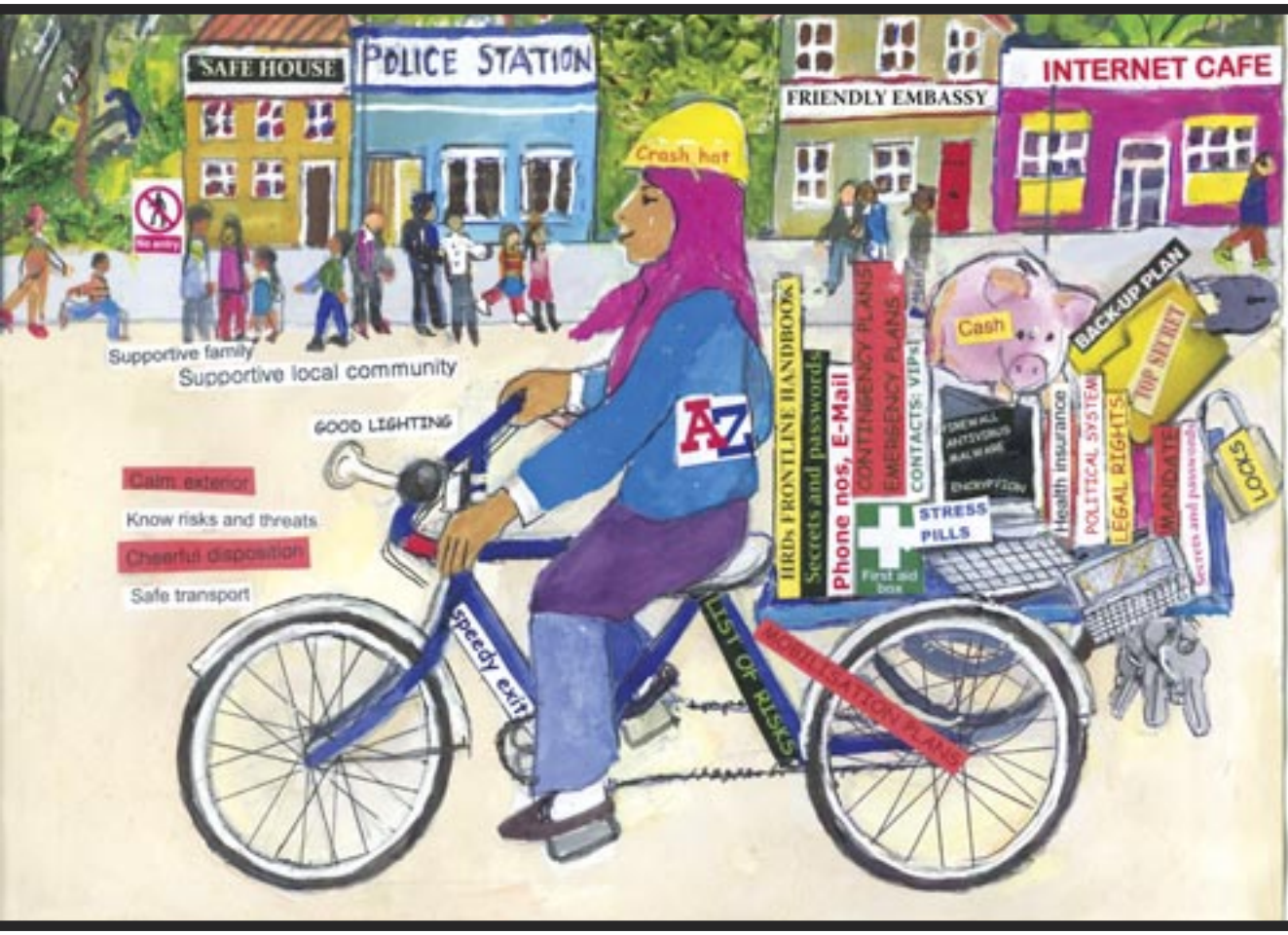
WORKBOOK ON SECURITY:

PRACTICAL STEPS FOR HUMAN RIGHTS DEFENDERS AT RISK



FRONT LINE DEFENDERS

APPENDIX 5

Check list: Office Security

This check list is not intended to be a blueprint for security. Your own context is the key determining factor. Consider the risks and threats you face, and any vulnerabilities you have in order to supplement and personalise this list.

1. Emergency Contacts
   - Is there a handy and up to date list with telephone numbers and addresses of other local NGOs, emergency hospitals, police, fire brigade and ambulance?

2. Technical and physical bounderies (external, internal and interior)
   - Check condition and working order of external gates / fences, doors to the building, windows, walls and roof
   - Check condition and working order of external lighting, alarms, cameras or video entrance phones
   - Check key procedures, including that keys are kept securely and code-labelled, assignment of responsibility for controlling keys and copies, and that keys and copies are in good working order. Make sure locks are changed when keys are lost or stolen, and that such incidents are logged
   - Do you have a special 'safe' room?
   - Can the sign with your office name on it be taken down in times of increased threat to reduce your vulnerability to attack?

3. Office personnel
   - Do you recruit only trustworthy people, including guards, and take up their references?
   - Are all personnel trained in the relevant security plans?
   - Do you have a plan in case the office is raided by the authorities, or other groups?
   - Do you operate a 'need-to-know' policy about the most sensitive work?
   - Do you maintain good dialogue with all staff, especially if you know they have financial problems or are under other pressures? (Disgruntled staff can make dangerous enemies.)
   - When someone leaves the organisation, do you change security measures, passwords, keys as appropriate?

4. Visitor Admission procedures and 'filters'
   - Are admission procedures in operation for all types of visitors? Are all staff familiar with them?
   - Do ask those staff members who usually carry out admission procedures if the procedures are working properly and what improvements are needed
   - Do staff know what to do if an unexpected parcel arrives? (eg isolate it, do not open, call authorities)
   - Do you note the names of visitors (including those attending meetings at your office)? If yes, is this information sensitive and how do you protect it? (for example by codes or encrypted files)

5. Information security (see also Appendix 14, Computer and Phone Security)
   - Do you carry out regular back-ups and keep the back-ups in a safe place outside of the office?
   - Do staff know not to leave any sensitive information on their desks?
   - Do you have a secure system for recording confidential information, eg about clients or witnesses?
   - Do you give your (physical and electronic) sensitive files secure names so they are not immediately identifiable?

6. Security in case of accidents
   - Check the condition of fire extinguishers, gas valves/pipes and water taps, electricity plugs and cables and elecricity generators (where applicable)

7. Responsibility and training
   - Has responsibility for office security been assigned? Is it effective?
   - Is there an office security training programme? Does it cover all the areas included in this review? Have all new staff members been trained? Is the training effective?