

August  
2014

# RESOURCE HUB FOR DEVELOPMENT COMMUNICATIONS POLICY

*Development for all Kenyans*

# **RESOURCE HUB FOR DEVELOPMENT**

## **COMMUNICATIONS POLICY**

Passed by the RHD Board on 27<sup>th</sup>  
August, 2014

## **1. INTRODUCTION**

- 1.1 RHD's communications facilities are provided by RHD and made available to its employees for the purposes of development initiatives. Use of our communications facilities is governed by the terms of this policy, and if our rules and procedures are not adhered to; then use of our facilities may be curtailed or withdrawn and disciplinary action may thereafter follow. Any breach of this policy may lead to disciplinary action being taken against an employee and serious breaches may lead to summary dismissal.
- 1.2 At RHD, communication plays an essential role in the conduct of our programmes. How you communicate with people not only reflects on you as an individual but also on us as an organization. We value your ability to communicate with colleagues, (people), our project donors and partners, and we invest substantially in information technology and communications systems which enable our employees to work more efficiently. We trust you to use them responsibly.
- 1.3 This policy applies to all individuals working for Resource Hub for Development (RHD), who use our communications facilities, whether (directors / departmental heads / Managers, Field Officers, Support Staff, partners / consultants], full-time, part-time or fixed-term employees, trainees, volunteers, contract staff or temporary staff.
- 1.4 Although the detailed discussion is limited to use of email and internet facilities, the general principles underlying all parts of this policy also apply to telephone communications, fax machines, copiers and scanners. Note that some elements of personal use of RHD's communications facilities are specifically addressed at items 3.3, 4.3 to 4.5, 9.4 and 9.5, and 10.5. Please read this policy carefully.

## **2. GENERAL PRINCIPLES**

- 2.1 You must use RHD's information technology and communications facilities sensibly, professionally, lawfully, and consistently with your duties, with respect for your colleagues and for the organization and in accordance with this policy and RHD's other rules and procedures.
- 2.2 All information relating to our project partners, donors and our programmes operations is confidential. You must treat our paper-based and electronic information with utmost care.

- 2.3 Particular care must be taken when using email, RHD's organization blog or internal message boards as a means of communication because all expressions of fact, intention and opinion in an email may bind you and/or RHD and can be produced in a court law in the same way as other kinds of written statements.
- 2.4 The advantage of the internet and email is that they are extremely easy and informal ways of accessing and disseminating information, but this means that it is also easy to send out ill-considered statements. All messages sent on email systems or via the internet should demonstrate the same professionalism as that which would be taken when writing a letter or a fax. You must not use these media to do or say anything which would be subject to disciplinary or legal action in any other context such as sending any discriminatory (on the grounds of a person's sex, race, disability, age, sexual orientation, religion or belief), defamatory, or other unlawful material (for example, any material that is designed to be, or could be construed as, bullying or harassment by the recipient). If you are in doubt about a course of action, take advice from your supervising authority (line manager/departmental head/partner).

### 3. **USE OF ELECTRONIC MAIL**

#### 3.1 **Generally**

- 3.1.1 Always use the email template which contains the appropriate disclaimer notice from RHD and do not amend this notice in any way.
- 3.1.2 Do not amend any messages received and, except where specifically authorized by the other person, do not access any other person's inbox or other email folders nor send any email purporting to come from another person.
- 3.1.3 It is good practice to re-read and check an email before sending.
- 3.1.4 If you copy an email to others, it may breach the Data Protection Act if it reveals all the recipients' email addresses to each recipient (e.g. in the case of marketing and mailing lists).

It can also breach duties of confidentiality (e.g. in the case of internal emails to members of staff benefit scheme). Accordingly, it may be appropriate to use the 'Bcc' (blind carbon copy) field instead of the 'Cc' (carbon copy) field when addressing an email to more than one

recipient. If in doubt, seek advice from your (line manager/departmental head/partner).

### **3.2 Organization use**

- 3.2.1 Each organization email should include the appropriate RHD programme/ business reference.
- 3.2.2 If the email message or attachment contains information which is time-critical, bear in mind that an email is not necessarily an instant communication and consider whether it is the most appropriate means of communication.
- 3.2.3 If you have sent an important document, always telephone to confirm that the email has been received and read.
- 3.2.4 In every instance, file a hard copy of any email (including any attachments) sent to or received from the organization partner, donor, volunteer, intern, consultant and other stakeholders before filing or deleting the electronic copy. The same applies to all internal email transmissions concerning programmes matters.
- 3.2.5 In light of the security risks inherent in some web-based email accounts, you must not email organization documents to your personal web-based accounts. You may send documents to a partner's web-based account if you have the express written permission to do so.
- 3.2.6 When you need to work on documents such as forms remotely, they can be saved to a disk or retrieved over the internet or via the organization's website.

### **3.3 Personal Use**

- 3.3.1 Although RHD's email facilities are provided for the purposes of our development programmes, we accept that you may occasionally want to use them for your own personal purposes. This is permitted on the condition that all the procedures and rules set out in this policy are complied with. Be aware, however, that if you choose to make use of our facilities for personal correspondence, you can expect very little privacy because RHD may need to monitor communications for the reasons given in item 9.1.

You will greatly increase the privacy of any personal email by complying with the procedures set out in item 3.3.3 below.

3.3.2 Under no circumstances may RHD's facilities be used in connection with the operation or management of any business other than that of RHD or a partner, donor/ initiatives of RHD unless express permission has been obtained from your (line manager/departmental head/partner).

3.3.3 All personal email you send from RHD's facilities must be marked PERSONAL in the subject heading, and all personal email sent or received must be filed in a separate folder marked "Personal" in your inbox should you wish to retain it after reading. Contact IT Support if you need guidance on how to set up and use a personal folder. All email contained in your inbox and your sent items box are deemed to be business communications for the purposes of monitoring (see item 9.4).

You must ensure that your personal email use:

- a) does not interfere with the performance of your duties;
- b) does not take priority over your work responsibilities;
- c) is minimal and limited to taking place substantially outside of normal working hours (i.e. during any breaks which you are entitled to or before or after your normal hours of work);
- d) does not cause unwarranted expense or liability to be incurred by RHD;
- e) does not have a negative impact on RHD in any way; and
- f) is lawful and complies with this policy.

3.3.4 By making personal use of our facilities for sending and receiving email you signify your agreement to abide by the conditions imposed for their use, and signify your consent to RHD monitoring your personal email in accordance with item 9 of this policy.

## 4. USE OF INTERNET

4.1 We trust you to use the internet sensibly. Bear in mind at all times that, when visiting a website, information identifying your PC may be logged. Therefore any activity you engage in via the internet may affect RHD.

- 4.2 We recognise the need for individuals to have to carry out some personal tasks during working hours, e.g. for internet research or online shopping, and this is permitted subject to the same rules as are set out for personal email use in item 3.3.4 of this policy. If these activities require additional software to be installed onto your PC then you should submit a request to IT Support who may be able to arrange this for you. Whenever you need to download software to enable you to access an online service you must obtain the express permission of the Manager of IT or the Technical Services Officer who will consider the request in line with RHD's policy.
- 4.3 You are strongly discouraged from providing your RHD's email address when using public websites for non-organization purposes, such as online shopping. This must be kept to a minimum and done only where necessary, as it results in you and RHD receiving substantial amounts of unwanted email.
- 4.4 Access to certain websites is blocked during normal working hours. If you have a particular business need to access such sites, please contact the Manager of IT or the Technical Services officer.

You must not:

- 4.4.1 introduce password-detecting software;
  - 4.4.2 seek to gain access to restricted areas of RHD's network;
  - 4.4.3 access or try to access data which you know or ought to know is confidential;
  - 4.4.4 intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software; nor
  - 4.4.5 carry out any hacking activities
  - 4.4.6 Use RHD's systems to participate in any internet chat room or post messages on any external website, including any message board or blog, unless expressly permitted in writing to do so by RHD.
- 4.5 For your information, breach of items 4.4.1 to 4.4.6 (inclusive) above, would not only contravene the terms of this policy but could in some circumstances also amount to the commission of an offence under the Computer Misuse Act 1990 and Kenya's Information and Communication Act 2013 which creates the following offences:
- 4.5.1 unauthorized access to computer material i.e. hacking;
  - 4.5.2 unauthorized modification of computer material; and
  - 4.5.3 Unauthorized access with intent to commit or facilitate the commission of further offences.

## 5. MISUSE OF RHD'S FACILITIES AND SYSTEMS

5.1 Misuse of RHD's facilities and systems, including its telephone, email and internet systems, in breach of this policy will be treated seriously and dealt with in accordance with RHD's disciplinary procedure. In particular, viewing, accessing, transmitting, posting, downloading or uploading any of the following materials in the following ways, or using any of RHD's facilities, will amount to gross misconduct capable of resulting in summary dismissal (among other disciplinary actions as provided in other RHD policies):

- 5.1.1 material which is sexist, racist, homophobic, xenophobic, pornographic, paedophilic or similarly discriminatory and/or offensive;
- 5.1.2 offensive, obscene, derogatory or criminal material or material which is liable to cause embarrassment to RHD and any of its staff or its partners or bring the reputation of RHD and any of its staff or its partners/ donors into disrepute;
- 5.1.3 any defamatory material about any person or organisation or material which includes statements which are untrue or of a deceptive nature;
- 5.1.4 any material which, by intent or otherwise, harasses the recipient;
- 5.1.5 any other statement which is designed to cause annoyance, inconvenience or anxiety to anyone;
- 5.1.6 any material which violates the privacy of others or unfairly criticises or misrepresents others;
- 5.1.7 confidential information about RHD and any of its staff or partners;
- 5.1.8 any other statement which is likely to create any liability (whether criminal or civil, and whether for you or RHD);
- 5.1.9 material in breach of copyright and/or other intellectual property rights;
- 5.1.10 online gambling; or
- 5.1.11 unsolicited commercial or advertising material, chain letters or other junk mail of any kind.

If RHD has evidence of the examples of misuse set out above it reserves the right to undertake a more detailed investigation in accordance with its disciplinary procedures.

## 6. SYSTEM SECURITY

- 6.1 Security of our IT systems is of paramount importance. We owe a duty to all of our staff and partners to ensure that all of our transactions are kept confidential. If at any time we need to rely in court on any information which has been stored or processed using our IT systems it is essential that we are able to demonstrate the integrity of those systems. Every time you use the system you take responsibility for the security implications of what you are doing.
- 6.2 RHD's system or equipment must not be used in any way which may cause damage, or overloading or which may affect its performance or that of the internal or external network.
- 6.3 Keep all confidential information secure, use it only for the purposes intended and do not disclose it to any unauthorized third party.
- 6.4 Keep your system passwords safe. Do not disclose them to anyone. Those who have a legitimate reason to access other users' inboxes must be given permission from that other user. IT Support staff will provide guidance on how to do this. If you have disclosed your password to anyone else (e.g. in response to a request from the IT staff) ensure that you change your password once the IT staff no longer need it. Contact IT Support for guidance on how to do this.
- 6.5 If a document is highly confidential or sensitive, you should mark it as "private and confidential" and password-protect the document itself. Bear in mind that documents which are NOT marked "private and confidential" can be accessed by all users of the network.
- 6.6 Copies of confidential information should be printed out only as necessary, retrieved from the printer immediately, and stored or destroyed in an appropriate manner.
- 6.7 You should not download or install software from external sources without having first received the necessary authorisation from (the IT department/line manager/ departmental head/ partner).
- 6.8 No external device or equipment, including discs and other data storage devices, should be run on or connected to RHD's systems without the prior notification to and approval of (the IT department/ line manager/ departmental head/ partner).
- 6.9 You should always exercise caution when opening emails from unknown external sources or where, for any reason, an email appears suspicious. The IT

department/ line manager/ departmental head/ partner should be informed immediately in such circumstances.

## **7. WORKING REMOTELY**

- 7.1 This part of the policy and the procedures in it apply to your use of our systems, to your use of our laptops, and also to your use of your own computer equipment or other computer equipment (e.g. partner's equipment) whenever you are working on RHD's programme/ assignment away from RHD's premises (working remotely).

When you are working remotely you must:

- 7.1.1 password protect any work which relates to RHD's work so that no other person can access your work;
  - 7.1.2 position yourself so that your work cannot be seen by any other person;
  - 7.1.3 take reasonable precautions to safeguard the security of our equipment, and keep your passwords secret;
  - 7.1.4 inform the police and our IT department (as appropriate) as soon as possible if either a laptop belonging to RHD in your possession or any computer equipment on which you do RHD's work, even if this is personal IT equipment, has been lost or stolen; and
  - 7.1.5 ensure that any work which you do remotely is saved on RHD's system or is transferred to our system as soon as reasonably practicable.
- 7.2 Pocket computers, mobile phones and similar hand-held devices are easily lost or stolen so you must password-protect access to any such devices used by you on which is stored any personal data of which RHD is a data controller or any information relating our programmes, partners and donors.

## 8. PERSONAL BLOGS AND WEBSITES

- 8.1 This part of the policy and procedures in it apply to content that you publish on the internet (e.g. your contributions to blogs, message boards and social networking or content-sharing sites) even if created, updated, modified or contributed to outside of working hours or when using personal IT systems.
- 8.2 RHD recognise that in your own private time you may wish to publish content on the internet. For the avoidance of doubt, such activities are expressly prohibited during work time or using RHD's systems.
- 8.3 If you post any content to the internet, written, vocal or visual, which identifies, or could identify, you as a member of RHD staff and/or you discuss your work or anything related to RHD or its business, customers or staff, RHD expects you, at all times, to conduct yourself appropriately and in a manner which is consistent with your contract of employment and with RHD's policies and procedures. It should be noted that simply revealing your name or a visual image of yourself could be sufficient to identify you as an individual who works for RHD.
- 8.4 If you already have a personal blog or website which indicates in any way that you work for RHD you should report this to your line manager/departmental head/partner.
- 8.5 If you intend to create a personal blog or website that will say that you work for RHD or in any way could identify you as someone who works for RHD then you should report this to your line manager/departmental head/partner.
- 8.6 If a blog posting clearly identifies that you work for RHD and you express any idea or opinion then you should add a disclaimer such as "these are my own personal views and not those of RHD".
- 8.7 The following matters will be treated as gross misconduct capable of resulting in summary dismissal (other matters will be added to this list):
  - 8.7.1 Revealing confidential information about RHD in a personal online posting. This might include revealing information relating to RHD's partners, business plans, policies, staff, financial information or internal discussions. Consult your manager if you are unclear about what might be confidential.
  - 8.7.2 Criticising or embarrassing RHD, its partner or its staff in a public forum (including any website). You should respect the corporate reputation of RHD and the privacy and feelings of others at all times. If you have a genuine complaint to make about a colleague or

workplace matter the correct procedure is to raise a grievance using RHD's grievance procedure.

8.7.3 Accessing or updating a personal blog or website from RHD's computers or during work time.

8.8 If you think that something on a blog or a website could give rise to a conflict of interest and in particular concerns issues of impartiality or confidentiality required by your role then this must be discussed with your line manager/departmental head/partner.

8.9 If someone from the media or press contacts you about your online publications that relate to RHD you should talk to your line manager/departmental head/partner before responding and RHD's press office must be consulted.

8.10 Online publications which do not identify the author as a member of RHD staff and do not mention RHD and are purely concerned with personal matters will normally fall outside the scope of RHD's communications policy.

## 9. **MONITORING OF COMMUNICATIONS BY RHD**

9.1 RHD is ultimately responsible for all communications but subject to that will, so far as possible and appropriate, respect your privacy and autonomy while working. RHD may monitor your business communications for reasons which include:

9.1.1 providing evidence of business transactions;

9.1.2 ensuring that RHD operations and procedures, policies and contracts with staff are adhered to;

9.1.3 complying with any legal obligations;

9.1.4 monitoring standards of service, staff performance, and for staff training;

9.1.5 preventing or detecting unauthorized use of RHD's communications systems or criminal activities; and

9.1.6 maintaining the effective operation of RHD's communications systems.

9.2 RHD will monitor telephone, email and internet traffic data (i.e. sender, receiver, subject; non-business attachments to email, numbers called and duration of calls; domain names of websites visited, duration of visits, and

files downloaded from the internet) at a network level (but covering both personal and business communications) for the purposes specified at item 9.1. For the purposes of your maintenance of your own personal privacy, you need to be aware that such monitoring might reveal sensitive personal data about you. For example, if you regularly visit websites which detail the activities of a particular political party or religious group, then those visits might indicate your political opinions or religious beliefs. By carrying out such activities using RHD's facilities you consent to our processing any sensitive personal data about you which may be revealed by such monitoring.

- 9.3 Sometimes it is necessary for RHD to access your communications during your absence, such as when you are away because you are ill or while you are on holiday. Unless your mailbox settings are such that the individuals who need to do this already have permission to view your inbox, access will be granted only with the permission of one of the persons authorized to grant such access in accordance with our policy "Access to Mailboxes".
- 9.4 Any emails which are not stored in your "Personal" folder in your mailbox and which are not marked PERSONAL in the subject heading will be treated, for the purpose of availability for monitoring, as business communications since we will have no way of knowing that they were intended to be personal. Therefore you must set up a rule to automate the routing of personal email to your personal folder – ask IT Support for guidance on how to do this. Furthermore, there is a risk that any person authorized to access your mailbox may have their own preview pane option as a default setting, which would reveal the content of any of your personal email not filed in your "Personal" folder, whether or not such email are marked PERSONAL. It is up to you to prevent the inadvertent disclosure of the content of personal email by filing your personal email in accordance with this policy. In particular, you are responsible to anybody outside RHD who sends to you, or receives from you, a personal email, for the consequences of any breach of their privacy which may be caused by your failure to file your personal email.
- 9.5 In certain very limited circumstances we may, subject to compliance with any legal requirements, access email marked PERSONAL. Examples are when we have reasonable suspicion that they may reveal evidence of unlawful activity, including instances where there may be a breach of a contract with RHD.
- 9.6 All incoming emails are scanned by a staff on behalf of RHD, using virus-checking software. The software will also block unsolicited marketing email (spam) and email which have potentially inappropriate attachments. If there is a suspected virus in an email which has been sent to you, the sender will automatically be notified and you will receive notice that the email is not going to be delivered to you because it may contain a virus.

## 10. DATA PROTECTION

- 10.1 As a member of RHD who uses our communications facilities, you will inevitably be involved in processing personal data for RHD as part of your job. Data protection is about the privacy of individuals, and is governed by the Kenya's Information and Communication Act 2013 and the Constitution of Kenya 2010. This defines, among others, terms as follows:
- 10.1.1 "data" generally means information which is computerised or in a structured hard copy form;
  - 10.1.2 "personal data" is data which can identify someone, such as a name, a job title, a photograph;
  - 10.1.3 "processing" is anything you do with data – just having data amounts to processing; and
  - 10.1.4 "data controller" is the person who controls the purposes and manner of processing of personal data – this will be RHD, in the case of personal data processed for the business.
- 10.2 Whenever and wherever you are processing personal data for RHD you must keep it secret, confidential and secure, and you must take particular care not to disclose them to any other person (whether inside or outside RHD) unless authorized to do so. Do not use any such personal data except as authorized by RHD for the purposes of your job.
- 10.3 The Kenya's Information and Communication Act 2013 gives every individual the right to see all the information which any data controller holds about them. Bear this in mind when recording personal opinions about someone, whether in an email or otherwise. It is another reason why personal remarks and opinions must be made or given responsibly, and they must be relevant and appropriate as well as accurate and justifiable.
- 10.4 Section 55 of the Data Protection Act provides that it is a criminal offence to obtain or disclose personal data without the consent of the data controller. "Obtaining" here includes the gathering of personal data by employees at work without the authorisation of the employer. You may be committing this offence if without authority of RHD: you exceed your authority in collecting personal data; you access personal data held by RHD; to control it or you pass them on to someone else (whether inside or outside RHD).
- 10.5 While RHD is a data controller of all personal data processed for the purposes of our business, you will be a data controller of all personal data processed in

any personal email which you send or receive. Use for social, recreational or domestic purposes attracts a wide exemption under the Data Protection Act, but if, in breach of this policy, you are using our communications facilities for the purpose of a business which is not RHD's business, and then you will take on extensive personal liability under the Data Protection Act.

- 10.6 To help you understand and comply with RHD obligations as a data controller under the Data Protection Act you may be offered, and you may also request, training. Whenever you are unsure of what is required or you otherwise need guidance in data protection, you should consult our Data Protection Officer [or any member of the data protection team]. RHD's privacy statements and information about our data protection policies can be found [on the RHD intranet.

## **11. COMPLIANCE WITH THIS POLICY**

- 11.1 Failure to comply with this policy may result in disciplinary action being taken against you under RHD's disciplinary procedures, which may include summary dismissal, and/or in the withdrawal of permission to use the organization's equipment for personal purposes. If there is anything in this policy that you do not understand, please discuss it with your line manager/departmental head/partner.
- 11.2 Please note that the procedures and policies outlined in this policy, and in any related policy, may be reviewed or changed at any time. You will be alerted to important changes and updates will be published on our intranet.