



Communication Protocols 2024

پالیسی ارتباطات- ۱۴۰۳ھ ش

OPHCD

Organization For Promotion of Health and Community Development



Developed on: December-2024

Table of Contents

ABOUT OPHCD:.....	2
1. INTRODUCTION, LEGAL STATUS.....	2
2. GENERAL PRINCIPLES:	3
3.1: VISION.....	3
3.2: MISION STATEMENT.....	3
4. OPHCD COMMUNICATION PROTOCOL.....	4
6. COMMUNICAITON TOOLS AND CHANNELS.....	11
7.USE OF THE INTERNET AND INTRANET:	12
8. MISUSE OF OPHCD'S FACILITIES AND SYSTEMS:	13
9. SYSTEM SECURITY:	13
10. WORKING REMOTELY:	14
11. PERSONAL BLOGS AND WEBSITES:	15
12. MONITORING OF COMMUNICATIONS BY OPHCD	16
13. DATA PROTECTION:	18
14.COMPLIANCE WITH THIS POLICY	19
15.POLICY REVIEW AND UPDATES	19
APPROVED BY:.....	20



ABOUT OPHCD:

1. INTRODUCTION, LEGAL STATUS

Organization for Promotion of Health & Community Development (OPHCD) is a non-government, non-profit, non-political, impartial and independent organization registered with:

- The NGOs Department of the Ministry of Economy of the Government of Islamic Republic of Afghanistan with license No. 4160

The organization established to serve the community and advocate for better coordinating and directing the available resources and activities for provision of quality services to the communities with an equitable manner. OPHCD, as a non-governmental organization committed for a joint mission with having dedicated and expert staff in public health, Water Sanitation and Hygiene, education, community development as well as volunteers who have been working in technical and managerial positions with national and international NGOs since more than one and half decade.

The members of the Board of Directors, senior Management Team (SMT) as well as the volunteers of the organization having appropriate experience, dedication and voluntarism which is a professional contribution to the health, education and development sector for achieving of more sustainable results.

The core staff of OPHCD have more than one and half decade of successful experience of being directly involved in **developing** different policies and strategies as well as **designing and implementation** of projects in the areas of health, WASH, education and community development sectors such as; Primary Health care (PHC), Basic Package of Health Services (BPHS), Essential Package of Health Services (EPHS), Water & Sanitation and Hygiene, Primary education and Literacy programs, Youth awareness and development, Public Nutrition, Emergency Preparedness and Response and Disaster Risk Reduction, trainings and coordination of different humanitarian Aids. Furthermore, the SMT and core Technical, Administration and Finance staff of the organization have up to date knowledge and rich experience of Grant Management, Project Management as well as conducting professional tasks of supportive Supervision, Monitoring, Evaluation, and Researches. Likewise, developing and on-time reporting (monthly, quarterly, annual, end of project and ad-hoc reports) to the donors and stakeholders, presenting the results of the aforementioned programs at the community, organizational, national and international levels are the expertise of the organization's technical and administrative staff.



3.1: VISION

An empowered society with sustainable and self-reliance health, social and economic stability at the community level.

3.2: MISSION STATEMENT

OPHCD, as a non-governmental organization is striving for well-being of the society with promotion of health and sustainable development of the communities through advocating for better coordinating and directing the national policies and strategies as well as available resources and activities for provision of quality health, educational, social safety, human right and social welfare, economic, environmental and development services to the communities with the focus on the women and children, drugs users, IDPs and other marginalized group of the society with an equitable manner.

2. GENERAL PRINCIPLES:

2.1: OPHCD'S communications facilities are provided by OPHCD and made available to users for the purposes of the business. A certain amount of limited and responsible personal use by users is also permitted. All 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 you and serious breaches may lead to summary dismissal.

2.2: At OPHCD, communication plays an essential role in the conduct of our business. 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, [clients/customers] and business contacts, and we invest substantially in information technology and communications systems which enable you to work more efficiently. We trust you to use them responsibly.

2.3: This policy applies to all individuals working for OPHCD who use our communications facilities, whether [directors / departmental heads/partners/consultants], full-time, part-time or fixed-term employees, trainees, contract staff, temporary staff, agency or home workers.

2.4: Although the detailed discussion is limited to the 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 OPHCD'S communication policy.

2.5: You must use OPHCD'S information technology and communications facilities sensibly, [professionally], lawfully, and consistently with your duties, with respect for your colleagues and OPHCD and following this policy and OPHCD'S other rules and procedures.

2.6: All information relating to our [clients/customers] and our business operations is confidential. You must treat our paper-based and electronic information with utmost care.

2.7: Many aspects of communication are protected by intellectual property rights which are infringed by copying. Downloading, uploading, posting, copying, possessing, processing and distributing material from the internet may be an infringement of copyright or of other intellectual property rights.

2.8: Particular care must be taken when using email, OPHCD'S company blog or internal message boards as a means of communication because all expressions of fact, 3 intention and opinion in an email may bind you and/or OPHCD and can be produced in court in the same way as other kinds of written statements.

2.9: 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 [line manager/departmental head/partner].

4. OPHCD COMMUNICATION PROTOCOL

1. Definition: An Organizational Communication Policy is a formal document that outlines the principles, guidelines, and procedures for internal and external communication within an organization. It serves as a framework to ensure that information is shared effectively, consistently, and responsibly across all levels of the organization and with external stakeholders.

2. Purpose and Objectives

Purpose: The purpose of an organizational communication protocol and policy is to establish clear guidelines and frameworks for effective, consistent, and professional communication within and outside the organization. This ensures that all stakeholders, employees, clients, partners, and the public receive accurate, timely, and respectful communication, thereby fostering a positive organizational culture and reputation.

3.1: Key Objectives of Communication Protocols and Policies:

- 1. To Promote Clear and Consistent Communication:** Standardize how information is shared to reduce confusion and misinterpretation, and to ensure messaging aligns with the organization's mission, vision, and values.



2. **To Enhance Efficiency and maintain professionalism:** Streamline communication processes to ensure timely and effective information exchange, and avoid duplication of efforts or gaps in information flow.
3. **To Protect the Organization's Reputation:** Outline approved channels and approaches for external communication to maintain a professional image, and to prevent the dissemination of incorrect, sensitive, or unauthorized information.
4. **To Foster transparency and Accountability:** Define roles and responsibilities for communication tasks, ensuring accountability among staff members, and clarify escalation pathways for resolving issues or reporting concerns.
5. **To Ensure Confidentiality and Security:** Establish rules for handling sensitive or confidential information to protect the organization and its stakeholders, and address the use of technology, such as email, social media, and messaging platforms, to safeguard against data breaches or misuse.
6. **To Improve Internal Collaboration and Engagement:** Encourage open, respectful, and constructive communication among team members, and to provide channels for feedback, suggestions, and conflict resolution.
7. **To Support Crisis Management:** Define procedures for managing communication during emergencies or crises, and to ensure that accurate information is disseminated promptly to mitigate potential harm.
8. **To Align with Legal and Ethical Standards:** Ensure compliance with laws, regulations, and ethical standards related to communication, and to avoid legal issues arising from miscommunication or misinformation, such as Data protection and privacy laws, Intellectual property and copyright standards, and ethical guidelines for professional conduct.

4.1 SCOPE OF OPHCD COMMUNICATION POLICY:

The scope of OPHCD communication policy defines the areas, individuals, and processes that the policy covers. It sets the boundaries for its application, ensuring clarity about where and how the policy is relevant. Typically, the scope encompasses the following:

1. Applicability: Who It Covers:

- All employees, including full-time, part-time, and temporary staff.
- Contractors, consultants, and volunteers representing the organization.
- Senior management, supervisors, and team leaders.
- External stakeholders (e.g., partners, vendors) involved in communication on the organization's behalf.



2. Where It Applies:

- Across all organizational departments, units, and locations (e.g., offices, remote work environments, project sites).

3. Communication Principles

- **Clarity and Conciseness:** Ensure messages are straightforward and to the point.
- **Consistency:** Use consistent messaging aligned with company values and goals.
- **Transparency:** Share necessary information openly, fostering trust.
- **Respect and Professionalism:** All communications should be courteous and respectful.
- **Inclusivity:** Language should be inclusive and free from bias.

4. Roles and Responsibilities

- **Senior Leadership:** Responsible for communicating strategic goals and fostering an open communication environment.
- **Managers:** Ensure clear communication of team goals and provide feedback to senior leadership.
- **Employees:** Responsible for participating actively, asking questions when needed, and adhering to communication standards.

5. TYPES OF COMMUNICATION PROTOCOLS

5.1: Internal Communication: OPHCD defines guidelines for email, meetings, memos, and digital and team collaboration tools (e.g., Teams) as the following for its internal communication.

- Employee interactions (emails, meetings, memos, instant messaging, reports).
- Communication between teams, departments, or management levels.
- Usage of communication tools (e.g., intranets, collaboration platforms).
- ❖ Mutual respect and sensitivity, as per the guidelines and code of conduct detailed in this institutional manual shall determine and guide the language and tone of all internal communications.
- ❖ It is recommended that all important decisions, communications, delegation, allocation even within teams and between teams should be documented in form of email communication to avoid confusion and misunderstandings and also to promote accountability.
- ❖ Supervisors should keep in mind that the tone and language of feedback in oral and written communication should be that of supportive supervision and mentoring rather than of fault-finding and policing.

OPHCD
Organization for Prevention of
Health & Community Development

5.1.1: Emails: OPHCD use emails for its formal internal communication which should be kept concise and actionable.

5.1.2: USE OF ELECTRONIC MAIL:

A: Generally

A.1: Always use the email template which contains the appropriate disclaimer notice from OPHCD and do not amend this notice in any way.

A.2: Do not amend any messages received and, except where specifically authorized by the other person, do not access any other person's in-box or other email folders nor send any email purporting to come from another person.

A.3: It is good practice to re-read and check an email before sending.

A.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 a 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].

B. Business use:

1. Each business email should include the appropriate OPHCD business reference.
2. If the email message or attachment contains information which is time critical, bear in mind that an email is not necessarily an instant 4 communication and consider whether it is the most appropriate means of communication.
3. If you have sent an important document, always telephone to confirm that the email has been received and read.
4. In every instance, file a hard copy of any email (including any attachments) sent to or received from the [customer/client] before filing or deleting the electronic copy. The same applies to all internal email transmissions concerning [customer/client] matters.
5. In light of the security risks inherent in some web-based email accounts, you must not email business documents to your personal web-based accounts. You may send documents to a [customer's/client's] web-based account if you have the [customer's/client's] express written permission to do so. [However, under no circumstances should you send price sensitive or highly confidential documents to a [customer's/client's] personal web-based email account, even if the [customer/client] asks you to do so.]
6. When you need to work on documents remotely, they can be saved to a disk or retrieved over the internet [via XXX website].

C. Personal Use:

1. Although OPHCD'S email facilities are provided for our business, we accept that you may occasionally want to use them for your 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 OPHCD may need to monitor communications for the reasons given in item 9.1.
2. You will greatly increase the privacy of any personal email by complying with the procedures set out in item 3.3.3 below.
3. Under no circumstances may OPHCD'S facilities be used in connection with the operation or management of any business other than that of OPHCD or a [customer/client] of OPHCD unless express permission has been obtained from your [line manager/departmental head/partner].
4. All personal emails you send from [XYZ CO'S] facilities must be marked PERSONAL in the subject heading, and all personal emails 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 emails contained in your inbox 5 and your sent items box are deemed to be business communications for the purposes of monitoring.

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 OPHCD;
 - (e) does not have a negative impact on OPHCD in any way; and
 - (f) is lawful and complies with this policy.
5. As with any correspondence made using OPHCD'S electronic facilities, you can delete personal emails from the live system, but they will have been copied (perhaps many times) onto the backup tapes and in that form will be retained indefinitely. It would be a very difficult, costly, and time-consuming exercise to sift all those tapes to delete an individual's email, and if we were to agree to attempt this, it would be at our convenience, and only on the basis that all the very considerable costs involved were paid in advance by the person making the request.
6. 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 OPHCD monitoring your email following item 9 of this policy.



5.1.2: Email signature:

5.1.2.1: For all email communication, including internal and external, the following standard signature template should be used:



Name: XNNX

Email: 0000000000000000 and Info@ophcd.org

+93 707825060

+93 747198740

Taimani Project, 4th District, Kabul-Afghanistan

ophcd.org



Be environmentally friendly -print this email only if you need to!

The information contained in this document is confidential information intended for your use only. If you are not the intended recipient, any dissemination, distribution or copying of this communication is strictly prohibited. If you receive this information in error, please notify us by emailing the original to the sender. Any views or opinions presented are solely those of the author and do not necessarily represent those of OPHCD unless otherwise specifically stated. If the content of this email is to become contractually binding, it must be made on paper and signed by a duly authorised representative of OPHCD.

5.1.2.2: Operation Manager is responsible for ensuring appropriate settings and configurations on all computers to enable standardisation of email signatures through IT officer.

5.1.3: Meetings: OPHCD ensures that each meeting has a clear Agenda, Meeting Attendance, and Meeting Minutes/purpose; and avoid from unnecessary meetings.

[5-Appendix 5th Template_Agenda.docx](#)

[6-Appendix Template_Meeting Minutes.docx](#)

[7- Appendix 7th Template_Meeting Attendance.xlsx](#)

In-Person or Virtual Meetings:

- At times, at the request of the OPHCD (staff, members) stakeholders, or beneficiaries a meeting may take place if either party feels that. this would be the most appropriate communication method.
- All the Meetings are conducted to discuss formal points of concern or well-being about stakeholders, Staff, or beneficiaries, all meetings must be agreed upon in advance.

- All the official meetings which are conducted without the meeting minutes are informal documents.

5.1.4: Telephone Communication (Calls, Messages):

- All telephonic communications including WHATSAPP Chats are informal documents, except in case it is made after the formal approval of the OPHCD's General Director.
- From telephone calls and email content will be saved electronically into the OPHCD's Archive profile.

5.1.5: Communication with the media:

No-one is authorized to interact with the media without prior written approval of the OPHCD's General Director.

1. Appendix 1st: [Letterhead.docx](#)
2. email Appendix 2nd, Info@ophcd.org,
3. Appendix 3rd: [Peshnihad.docx](#)
4. Aastellas Appendix 4th: [Aastilam.docx](#)

5.2: External Communication Protocols: Covers interactions with clients, vendors media, public relations, and social media use.

- Media relations (press releases, interviews).
- Public statements and speeches by organizational representatives.
- Marketing and promotional content (advertisements, brochures, social media posts).
- Correspondence with stakeholders, clients, and partners.
- ✓ Only staff at the level of **L1** is authorised in organization to sign and send external communication.
- ✓ Staff at the level of **L2** only are authorised to sign and send communications related to their functional project areas to their counterparts in the country partner organisations.
- ✓ No person at the levels of **L3** and below can send any external communication without prior written permission and clearance from their respective supervisors.
- ✓ No deviations to the above protocol shall be accepted under any circumstances.
- ✓ All hard and soft communications should be conducted from the organization official address



5.3: Emergency Communication: Define a clear chain of command and standardized process for crisis and emergency communication to ensure that information is reported, verified, approved, and communicated promptly, accurately, and consistently.

The protocol shall establish designated focal points and escalation levels for emergencies, including security incidents, operational disruptions, safeguarding/PSEA concerns, reputational risks, serious incidents, natural disasters, and other events that may affect OPHCD staff, beneficiaries, assets, programs, or organizational reputation.

The Emergency Communication process shall include:

- **Immediate Reporting:** Any staff member identifying an emergency shall immediately report it to the designated supervisor or focal point through the approved communication channel.
- **Chain of Command:** Information shall move through the established reporting line from Field/Facility Level → Provincial/Field Management → Head Office → Senior Management/Head of Organization → Board of Trustees, as applicable.
- **Verification:** The responsible focal point shall verify available facts before external communication, while avoiding unnecessary delays where immediate life-saving or safety related communication is required.
- **Crisis Communication Team:** OPHCD shall designate responsible personnel for coordination, information management, media communication, donor communication, safeguarding matters, and management decision-making.
- **Single Source of Official Information:** Only authorized spokespersons or personnel designated by OPHCD management may issue official external statements or communicate with media on behalf of the organization.
- **Internal Communication:** Staff shall receive timely, factual, and need-to-know information through approved channels to reduce misinformation, confusion, and duplication.
- **External Communication:** Communication with donors, government authorities, UN/cluster partners, communities, media, and other stakeholders shall follow applicable contractual, legal, safeguarding, and organizational requirements.
- **Confidentiality and Data Protection:** Sensitive information, personal data, identities of affected persons, security information, and safeguarding-related details shall be protected and shared strictly on a need-to-know basis.
- **Documentation:** All significant crisis communications, decisions, approvals, notifications, and follow-up actions shall be recorded in the OPHCD Crisis Communication Plan & Response Tracker.
- **Post-Crisis Review:** Following a major emergency, OPHCD shall conduct a communication debrief to identify lessons learned, gaps, corrective actions, and improvements to the communication protocol, The OPHCD Proposed Crisis Communication plan as annex ,[Crisis Communication Plan Annex A00-5.xlsx](#)

6. COMMUNICAITON TOOLS AND CHANNELS

OPHCD Specifies and approved the following platforms and methods covered by the communication policy:

- Digital channels (emails, social media, websites, messaging apps).
- Print media (official documents, brochures, newsletters).
- Verbal communication (meetings, presentations, phone calls).
- Define when and how each channel should be used.

7.USE OF THE INTERNET AND INTRANET:

- 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 OPHCD.
- We recognize the need for individuals to have to carry out some personal tasks during working hours, e.g., for internet banking or online shopping, and this is permitted subject to the same rules as are set out for personal email use in 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 IT or the Technical Services Manager] who will consider the request in line with OPHCD'S policy.]
- You are strongly discouraged from providing your OPHCD email address when using public websites for non-business purposes, such as online shopping. This must be kept to a minimum and done only where necessary, as it results in you and OPHCD receiving substantial amounts of unwanted emails.
- [Access to certain websites is blocked during normal working hours. If you have a particular business need to access such sites, please contact [the Director of IT or the Technical Services Manager].

You must not:

- ✓ introduce packet-sniffing or password-detecting software;
- ✓ seek to gain access to restricted areas of OPHCD'S network;
- ✓ access or try to access data which you know or ought to know is confidential;
- ✓ intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software; nor
- ✓ carry out any hacking activities



- ✓ [use OPHCD'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 OPHCD]

8. MISUSE OF OPHCD'S FACILITIES AND SYSTEMS:

- ❖ Misuse of OPHCD'S facilities and systems, including its telephone, email and internet systems, in breach of this policy will be treated seriously and dealt with by OPHCD's disciplinary procedure. In particular, viewing, accessing, transmitting, posting, downloading, or uploading any of the following materials in the following ways, or 7 using any of OPHCD'S facilities, will amount to gross misconduct capable of resulting in summary dismissal (this list is not exhaustive): material which is sexist, racist, homophobic, xenophobic, pornographic, paedophilic or similarly discriminatory and/or offensive;
- offensive, obscene, derogatory or criminal material or material which is liable to cause embarrassment to OPHCD and any of its staff or its [customers/clients] or bring the reputation of OPHCD and any of its staff or its [customers/clients] into disrepute;
- any defamatory material about any person or organisation or material which includes statements which are untrue or of a deceptive nature;
- any material which, by intent or otherwise, harasses the recipient;
- any other statement which is designed to cause annoyance, inconvenience or anxiety to anyone;
- any material which violates the privacy of others or unfairly criticises or misrepresents others;
- confidential information about OPHCD and any of its staff or [customers/clients];
- any other statement which is likely to create any liability (whether criminal or civil, and whether for you or OPHCD);
- material in breach of copyright and/or other intellectual property rights;
- online gambling; or
- unsolicited commercial or advertising material, chain letters or other junk mail of any kind.

If OPHCD 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.

9. SYSTEM SECURITY:

1. Security of our IT systems is of paramount importance. We owe a duty to all of our [customers/clients] to ensure that all of our business 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.

2. OPHCD'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.
3. Keep all confidential information secure, use it only for the purposes intended and do not disclose it to any unauthorized third party.
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 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.
5. [If a document is highly commercially confidential or price 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. [Copies of confidential information should be printed out only as necessary, retrieved from the printer immediately, and stored or destroyed in an appropriate manner.]
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].
8. No external device or equipment, including discs and other data storage devices, should be run on or connected to OPHCD'S systems without the prior notification to and approval of [the IT department/line manager/departmental head/partner]
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.

10. WORKING REMOTELY:

- ❖ 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. client's equipment) whenever you are working on OPHCD'S business away from OPHCD'S premises (working remotely).

When you are working remotely you must:

- ✓ password protect any work which relates to OPHCD'S business so that no other person can access your work;
- ✓ position yourself so that your work cannot be seen by any other person;

- ✓ take reasonable precautions to safeguard the security of our equipment, and keep your passwords secret;
 - ✓ inform the police and our IT department (as appropriate) as soon as possible if either a OPHCD laptop in your possession or any computer equipment on which you do OPHCD'S work, even if this is personal IT equipment, has been lost or stolen; and
 - ✓ ensure that any work which you do remotely is saved on OPHCD'S system or is transferred to our system as soon as reasonably practicable.
- ❖ 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 OPHCD is a data controller or any information relating our business, our clients or their business.

11. PERSONAL BLOGS AND WEBSITES:

- 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.
- OPHCD 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 OPHCD'S systems.
- If you post any content to the internet, written, vocal or visual, which identifies, or could identify, you as a member of OPHCD staff and/or you discuss your work or anything related to OPHCD or its business, customers or staff, OPHCD expects you, at all times, to conduct yourself appropriately and in a manner which is consistent with your contract of employment and with OPHCD'S policies and procedures. It should be 10 noted that simply revealing your name or a visual image of yourself could be sufficient to identify you as an individual who works for OPHCD.
- If you already have a personal blog or website which indicates in any way that you work for OPHCD you should report this to your [line manager/departmental head/partner].
- If you intend to create a personal blog or website that will say that you work for OPHCD, or in any way could identify you as someone who works for OPHCD then you should report this to your [line manager/departmental head/partner].



- If a blog posting clearly identifies that you work for OPHCD 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 OPHCD".

The following matters will be treated as gross misconduct capable of resulting in summary dismissal (this list is not exhaustive):

- ✓ Revealing confidential information about OPHCD in a personal online posting. This might include revealing information relating to OPHCD'S clients, business plans, policies, staff, financial information or internal discussions. Consult your manager if you are unclear about what might be confidential.
- ✓ Criticising or embarrassing OPHCD, its clients or its staff in a public forum (including any website). You should respect the [corporate] reputation of OPHCD 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 OPHCD'S grievance procedure.
- ✓ [Accessing or updating a personal blog or website from OPHCD'S computers or during work time.]
- 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].
- If someone from the media or press contacts, you about your online publications that relate to OPHCD you should talk to your [line manager/departmental head/partner] before responding and OPHCD'S press office must be consulted.
- Online publications which do not identify the author as a member of OPHCD staff and do not mention OPHCD and are purely concerned with personal matters will normally fall outside the scope of OPHCD'S communications policy.

12. MONITORING OF COMMUNICATIONS BY OPHCD:

- OPHCD is ultimately responsible for all business communications but subject to that will, so far as possible and appropriate, respect your privacy and autonomy while working. OPHCD may monitor your business communications for reasons which include:
 - ✓ providing evidence of business transactions;
 - ✓ ensuring that OPHCD'S business procedures, policies and contracts with staff are adhered to;
 - ✓ complying with any legal obligations;



- ✓ monitoring standards of service, staff performance, and for staff training;
 - ✓ preventing or detecting unauthorized use of OPHCD'S communications systems or criminal activities; and
 - ✓ maintaining the effective operation of OPHCD's communications systems.
- OPHCD 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 OPHCD'S facilities you consent to our processing any sensitive personal data about you which may be revealed by such monitoring.
 - Sometimes it is necessary for OPHCD to access your business 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"].
 - 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 12 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 is 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 OPHCD 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.
 - 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 OPHCD.
 - [All incoming email are scanned by [XXX] on behalf of OPHCD, 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.]

13. DATA PROTECTION:

- As a member of OPHCD who uses our communications facilities, you will inevitably be involved in processing personal data for OPHCD as part of your job. Data protection is about the privacy of individuals, and is governed by the Data Protection Act 1998. This Act defines, among others, terms as follows:
 - ✓ "data" generally means information which is computerised or in a structured hard copy form;
 - ✓ "Personal data" is data which can identify someone, such as a name, a job title, a photograph;
 - ✓ "processing" is anything you do with data – just having data amounts to processing; and
 - ✓ "Data controller" is the person who controls the purposes and manner of processing of personal data – this will be OPHCD, in the case of personal data processed for the business.
- Whenever and wherever you are processing personal data for OPHCD 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 OPHCD) unless authorized to do so. Do not use any such personal data except as authorized by OPHCD for the purposes of your job. If in doubt get help from our Data Protection Officer or your [line manager/departmental head/partner].
- The Data Protection Act 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.
- For your information, 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 OPHCD: you exceed your authority in collecting personal data; you access personal data held by OPHCD; to control it or you pass them on to someone else (whether inside or outside OPHCD).
- While OPHCD 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 OPHCD'S business, then you will take on extensive personal liability under the Data Protection Act.

- To help you understand and comply with OPHCD'S 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]. [OPHCD'S privacy statements and information about our data protection policies can be found [on the XYZ CO intranet]].

14.COMPLIANCE WITH THIS POLICY

- Failure to comply with this policy may result in disciplinary action being taken against you under OPHCD'S disciplinary procedures, which may include summary dismissal, and/or in the withdrawal of permission to use the firm'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].
- 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].

We intend that all communication at the OPHCD level should:

- ✓ Keep all the stakeholders, staff, and beneficiaries well informed by the official letters, Appendix 1st, email Appendix 2nd, Request letter (Pashnihad) Appendix 3rd, and Aastellas Appendix 4th of the OPHCD's, standards.
- ✓ All the information related to the OPHCD should be open, honest, ethical, and professional.
- ✓ Use the Afghanistan's official national languages (Pashto & Dari) in all the communication official.
- ✓ Use the English language (united) need-based and donor and stakeholder's requirements which be easily understood by all.
- ✓ Use Times New Roman font for all English-language documents and Bahij Nazanin font for all documents written in national languages.



15.POLICY REVIEW AND UPDATES

Version No:	Approval date:	Approved by:	Change:
001	Jan,2021	Board of Trustee General Director	
002	December,2024	Board of Trustee General Director	

Signature.....

Date.....2024.....

APPROVED BY:

After the review of the policy, on behalf of the OPHCD Board of Trustees, the said manual is hereby approved and ready to be implemented henceforth.

Reviewed and Approved: Board of Trustee

Effective from Qawas, 1403 (December-2024)

