PARTNERS IN JUSTICE INTERNATIONAL

PJI DATA HANDLING AND PROTECTION POLICY

Table of Contents

General provisions

1. When carrying out work for or on behalf of Partners in Justice International (PJI), all team members involved in any capacity are obliged to comply with the laws and regulations in force in all countries in which PJI operates. In addition, they are required to comply with this Data Handling and Security Policy and other internal regulations and circulars.

2. The pursuit of PJI's interests cannot justify, in any event, conduct that does not respect the applicable laws.

3. This Policy concerns data handling and security and covers your use of PJI computers, files, email systems and software. It also covers the use of the Internet and computer networks available in PJI's offices, including when these are accessed using personal or third-party computers.

Internet and email usage

4. We seek a workplace that is free of harassment, sensitive to the diversity of our counterparts and staff, and true to the principles underpinning our work. Therefore, staff members, consultants, interns, and volunteers are not allowed to use computers and email in ways that are disruptive, offensive to others, or harmful to the dignity or morale of the organisation.

5. At PJI you may not use computers and email for ethnic slurs, racial comments, or anything that another person might take as harassment or disrespect of any kind. You also may not display, download, or email pornographic or otherwise offensive or degrading images or messages, unless those are expressly part of your work. If you are unsure about what is expressly part of your work, ask your supervisor for further guidance and clarification.

6. Everyone must respect the obligation of confidentiality. Information you acquire as part of PJI, irrespective of whether it is received or sent through email, is covered by the PJI confidentiality policy. This means that PJI staff, interns, consultants, and volunteers undertake to treat all information they acquire during their work as confidential. PJI staff, interns, consultants, and volunteers are not at liberty to divulge or discuss such information with anybody outside PJI, except as necessary for the fulfilment of their work or with the express permission of PJI, which should be sought in writing from your supervisor. Where such permission is granted, you must acknowledge the role of PJI in any publication. If you are unsure about what is considered necessary for the fulfilment of your work, ask your supervisor for further guidance and clarification.

7. During your work, you may have access to the internet through PJI networks or other networks provided to you because of your work with PJI, for example in field missions. This policy explains our guidelines for using the Internet. All Internet data that is written, sent, or received electronically, related to PJI's activities, is part of official PJI records. That means that we can be legally accountable for content and we may be required to show that information to law enforcement or other parties. Therefore, you should always make sure that the business information contained in Internet email messages and other transmissions is accurate, appropriate, ethical and legal. This policy applies whenever you are undertaking PJI work or using PJI-provided networks, also in the event that you are using private property or the property of a third party.

8. Examples of unacceptable use include, but are not limited to:

    a) Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via PJI's email service.

b) Using computers to perpetrate any form of fraud, and/or software, film, music or other piracy or copyright infringement.

c) Stealing, using, or disclosing someone else's password without authorisation.

d) Sharing confidential material, trade secrets, or proprietary information outside of the organisation.

e) Hacking into unauthorised websites.

f) Sending or posting information that is defamatory to the company, its products/services, colleagues and/or partners/donors.

g) Introducing malicious software onto the company network and/or jeopardising the security of the organisation's electronic communications systems.

h) Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities.

i) Passing off personal views that contradict PJI's policies and priorities as representing those of the organisation.

9. If you are unsure about what constitutes acceptable Internet usage, ask your supervisor for further guidance and clarification.

Cyber & Digital Security Protocols

14. PJI recognizes the potential for individuals, organizations, states, and non-state actors to breach PJI's cyber and digital security. Potential threats include break-in and theft of computers and information, theft of laptops or phones (in the field or at home), hacking into PJI's main server or specific desktop files, and/or hacking emails or texts on laptops or mobile devices. In order to mitigate each of these threats, PJI has protocols in place to protect all of its information, especially its program files. In addition, PJI requires that those who have access to the PJI server abide by digital security best practices, including maintaining up-to-date security software as outlined below.

15. At PJI, you may be connected to a network that allows you access to the PJI server or PJI files, whether cloud-based or not, whether you are using a PJI computer or your own. In order to protect the network from viruses and spyware, you agree to use at a minimum antivirus software, spyware, and a virtual private network (VPN). You are also required to update these programs on a regular basis. PJI will provide you with the software if you have any difficulties locating it. Please *do not* install more than one spyware or anti-virus program, as this may cause the program(s) to malfunction. This is of critical importance not just for you, but for the entire network, including the PJI server. Update the programs and run a scan at least once per week. If you find a virus, unplug the network cable of your computer (or switch off the wi-fi) and immediately notify your supervisor, so they can help determine what action will need to be undertaken by the rest of the office. If you find spyware, you can simply "fix" the problem using the regular spybot function.

16. As an additional layer of security, you also agree to register for two-factor authentication for your PJI email and cloud server account. PJI will provide you with the information you need to set this up. If a hacker manages to get a password, the two-step verification will prevent access. Each time you log onto a new device, a unique code will be texted to your cell phone. The hacker will not have the code and will be stopped from logging in, and you will know that your password

has been compromised because you will get the text message. Note that if you are in an area or country where cell phone access is limited, you may not be able to rely on receiving such texts. To work around this, consider registering a Google Voice account that can receive texts via email. Or carry a Yubikey that can be used as an alternative form for two-step verification. Or generate a series of authentication codes before travelling and print them out or keep them in some other way, to be able to log in without getting a text. For those who frequently clear "cookies" and cache from your web browser, you will be prompted for the security code and need to receive the text message each time you log on after clearing the cookies.

17. PJI recommends that if you do not already have it, install anti-tracking and safe website (SSL) detection software on your internet browser and cell phone, as well as software to assist you in keeping your digital information safe by deleting unnecessary files, temporary files, and browser cache files. PJI will provide you with the software if you have any difficulties locating it.

14. Take care not to fall victim to 'phishing' or "spear fishing" emails that could enable hackers to gain access to passwords, confidential files, or other information. Such attacks typically come in an email that appears to be from a legitimate source – a bank, an IT department, an email provider, or a friend. There will be a link along the lines of "I've shared a file with you", or "your bank account needs to be verified." Clicking on the link takes the user to a realistic-looking login page, using stolen graphics from a legitimate site. Once login information is entered, it is sent directly to the hacker, and they use it to break into the account. 'Spear phishing' is just more targeted phishing. Spear phishing happens when the scammers have researched their target by looking at social media sites, the organization's web site, etc. to send a targeted scam email addressed personally, forging the email headers to appear that it came from a colleague, with references to things that sound legitimate. The target of the attack is a lot more likely to fall for a scam if it is personalized. To check the validity of suspicious emails, you can hover your cursor over the link or button that takes you to the malicious page. This will allow you to view the true URL of the target site. If it is not familiar, do not open or download the email.

15. You may use a mobile phone or mobile phone application in the course of your work for PJI. You must ensure that especially sensitive communications are also fully encrypted, whether sent by email or text. PJI will provide you with the software if you have any difficulties locating it. This protocol applies unless local laws or other considerations necessitate a different approach. Some countries make it illegal to encrypt information. Some clients may fear increased surveillance if they use encryption technology. In such situations, team members must determine how best to communicate sensitive information.

16. You may need to use a flash drive to store or transport sensitive data in a flash drive. Only pre-encrypted flash drives should be used for this purpose. PJI will provide you this equipment if you need it.

17. Please take care in what apps or similar programs you allow to access your data, whether on your phone or computer. Some tools can be set up to access or push data into your account. Inform yourself about any security implications before you grant any such access. When traveling in higher risk countries and situations, PJI may provide you with a project-specific laptop and cell phone, in which case downloading of apps and similar programs will be restricted. Such laptops and cell phones will not be re-used for different projects but rather wiped and resold to avoid recognition or tracking of the IP address.

Email and Chat lists

22. PJI may develop email lists, including "all@partnersinjustice.org", which would be designed to make it easy to distribute information to a wide range of people. If you are a user of a mailing list,

you will generally be able to post to it (i.e., send an email), reaching automatically all the inscribed users. As a user of that mailing list you will receive all the emails sent to it, which will display the name of the list in the object, contained in squared parenthesis (e.g. [all]).

23. PJI uses group chat lists, via end-to-end encrypted text apps, which lists are designed to make it easy to distribute information to a wide range of people. If you are a member of a chat group, you will generally be able to post to it (i.e., send a text), reaching all the group members automatically. As a user of the group chat, you will receive all the texts that are sent to it. The group name will identify the thread.

24. PJI may develop "permanent" mailing or chat lists, which are basically used for internal communications, reports, etc. In addition, PJI may develop specific project-related mailing and chat lists, created in the light of a forthcoming event and which would be deleted after the event (conference, mission, etc.). Sending information through this type of mailing or chat list has the advantage of sharing information easily and consistently within a team without the risk of missing someone.

25. Please note that when you reply to a message sent to a mailing or chat list, your reply may go to the whole list, not only to the original sender. If you want to write to the sender, you can "forward" the email to them or text them individually.

Email protocols

26. Everyone at PJI receives and sends many, many emails per day. In general, it is wise to reply to emails within 24 hours. If this is not possible, it is a good idea to send an acknowledgment to the sender, including for internal emails. This helps everyone keep track of where things are and lets people know whether their emails were received or not.

27. When replying substantively to an email, make sure that you have answered all the points raised in the email, even if it is to say you need to get back to the sender (then remember to get back to them). Before sending, particularly for complicated emails, put them aside for a few minutes, then re-read from the perspective of the person receiving the email to make sure things are clear and courteous. If in doubt, ask someone else to take a look. Always run the spell check through emails before sending.

ANNEX I: PROCEDURE FOR KNOWN OR SUSPECTED VIOLATIONS OF APPLICABLE LAW AND/OR PJI POLICIES

Pursuant to paragraph 9 of this Policy, this Annex sets out the procedure in the case of known or suspected violations of applicable law and/or PJI policies.

1. The Director, Co-Director, and/or the Board will determine whether there are reasonable grounds to believe that the applicable law or this Policy have been violated; whether there is a need for steps additional to those contained in this Policy to ensure the security of PJI's information system (e.g. virus checking); or whether the criteria in REGULATION (EU) 2016/679are satisfied.1

2. When a positive determination is made pursuant to paragraph 1, the Director, Co-Director or Treasurer will determine whether there is a need for individual monitoring or access to the email of staff member, intern, consultant or volunteer.

3. The Director Co-Director or Treasurer or a designated representative will provide written notification to the relevant staff member, intern, consultant or volunteer, containing the following information:

a) the determination referred to in paragraph 1 of this annex and the factual basis for such determination;

b) the determination referred to in paragraph 2 of this annex and the reasons for such determination;

c) the PJI staff member responsible for following the issue. Usually this will be the Director, Co-Director or Treasurer, except where there may be a conflict of interest or some other reason for a different staff member to handle the dossier;

d) a request for input from the staff member, intern, consultant or volunteer regarding the situation, including any objections to the designation of the PJI staff member referred to in sub-paragraph (c);

e) the right of the staff member, intern, consultant or volunteer to request a hearing within 7 calendar days of receipt of the notification; and

f) any other relevant information.

4. If the staff member, intern, consultant or volunteer requests a hearing pursuant to sub-paragraph 3(e) of this annex, the hearing will be convened by the Director, Co-Director or Treasurer, or a designated representative, within 7 calendar days of receipt of the request.

5. If, after considering the input of the staff member, intern, consultant or volunteer and/or the results of the hearing, the Director, Co-Director or Treasurer shall determine whether there is a need to proceed with individual monitoring or access to the email of staff member, intern, consultant or volunteer and how such monitoring or access shall be done.

---

[1] For example, monitoring or access is necessary for compliance with a legal obligation to which PJI is subject (article 6(c)); or monitoring or access is necessary for the legitimate interests of PJI, except where such interests are overridden by the interests for fundamental rights or freedoms of the staff member, intern, consultant or volunteer (article 6(f)). Other criteria in article 6 may also be applicable. The Directive is available online at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504.

6. The Director, Co-Director or Treasurer, or a designated representative, shall notify the staff member, intern, consultant or volunteer of the determination referred to in paragraph 5 of this annex within 14 calendar days of receipt of the input referred to in sub-paragraph 3(d) or the hearing referred to in paragraph 4, whichever is later.

7. The staff member, intern, consultant or volunteer has the right to consent to individual monitoring or access to their email, in which case such monitoring or access shall proceed according to the terms of the determination referred to in paragraph 5 of this annex.

8. The staff member, intern, consultant or volunteer has the right not to consent to individual monitoring or access to their email, or to withdraw consent provided pursuant to paragraph 7 of this annex at any time, in which case the Director, Co-Director or Treasurer, or his or her designated representative, may seek to implement such monitoring or access through legal processes contained in the applicable law, including seeking a court order for such monitoring or access.

Annex II: Explanatory Note

A. When is the Policy intended to cover the use of which computers?

- The Policy covers instances where PJI team members such as directors, legal fellows, interns, consultants and volunteers use computers provided by PJI, whether in the field or in an PJI office.
- The Policy covers instances where PJI team members use their own computers for PJI work or through PJI-provided networks.
- The Policy does not cover PJI team members using their own computers on their own time through a network not provided by PJI.

B. Why does the Policy cover the use of private computers?

The Policy covers the use of private computers only when they are used for PJI work or through PJI-provided networks. It is possible that PJI would be liable for acts undertaken by PJI team members in their working capacity, irrespective of whether they are using private or PJI computers. It is for this reason that the Policy extends to the use of private computers when used for PJI work or through PJI-provided networks and notes that in the event of a breach of applicable law or PJI policies, PJI may require access to personal email accounts. It only covers access to personal email accounts in the event they are used for PJI work.

C. Why does the Policy prohibit using computers to perpetrate any form of fraud, and/or software, film, music or other piracy or copyright infringement?

The Policy prohibits this kind of activity using PJI computers or PJI-provided networks because it is illegal and PJI could be liable for the actions of its team members in this respect. However, it only covers this kind of activity done when using PJI computers or PJI-provided networks, as provided for in the description of the applicability of the Policy. While PJI encourages its team members to abide by the law, what people do on their own time using their own property is their own business.

D. What does "hacking into unauthorised websites" mean?

In the computer security context, a hacker is someone who seeks and exploits weaknesses in a computer system or computer network. When this is done without authorisation, it could constitute a criminal offence. If it is done using PJI computers or PJI-provided networks, PJI could be liable. Hence, it is prohibited.

E. What does "passing off personal views as that of the organisation" mean?

The issue here is that it is not appropriate for PJI team members to make representations to third parties regarding the views of the organisation that do not comply with the organisation's policies and priorities. An example would be if someone said that PJI supported all aspects of the Iraq Tribunal including its penalties, which included the death penalty. It would not cover situations where interlocutors ask for opinions on which team

members – and senior team members in particular – do not have time to consult internally but which follow PJI policies and priorities (in which case, if team members are unsure about whether what they say reflects PJI policies and priorities, it is wise to note that the issue has not been discussed internally).