THE PRINCE PHILIP DENTAL HOSPITAL

Guidelines on the Use of Hospital Windows Accounts, E-mail Accounts, Access through Personal Electronic Devices and Remote Desktop Connection

PURPOSE

The purpose of these Guidelines are to set out the general rules when using the Hospital's own Windows, email accounts and network share access. These Guidelines is to be read in conjunction with the following relevant documents:

- Section E6 of Human Resources Manual of the Hospital;
- Service Manual of the IT Office;
- Guidelines on Management of the Administrator Account of an Application System;
- Guidelines on the Appropriateness to use the Hospital-owned Portable Electronic Storage;
- Guidelines on blocking the websites containing pornography, inappropriate and offensive material;
- Guidelines on Third Party's Remote Access to Computer Systems and Network of The Prince Philip Dental Hospital;

plus the useful kits of

- Application for the Windows and Email Accounts;
- Application for the Remote Desktop Connection;
- Tips to write an email;

SCOPE

2. These Guidelines shall apply to all relevant staff members of the Hospital.

GENERAL PRINCIPLES

3. Hospital staff members with Hospital email accounts should observe the provisions under Part III "*General Security for Server Room as well as of Using Hospital Computers, Emails and Application Software*" as well as Clause 14 (h) of Section E6 of the Human Resources Manual.

4. Hospital staff members are responsible for the safekeeping of the assigned Hospital accounts and for all activities performed using these accounts.

Last reviewed in September 2021
Edited by IT Office of PPDH

APPROPRIATE USE OF EMAIL ACCOUNT

5. Hospital does not allow the use of an individual's private email accounts for any official businesses. Meanwhile, Hospital staff members should not send bulk, spam and unsolicited email through their PPDH official email account.

6. All emails and documents contained in the Network Share Access are treated as Hospital's property. Hospital staff members should not delete them deliberately, except for those phishing emails or with justifiable reasons. They should not distribute, disseminate the images, text or material that might be appeared to be indecent, pornographic, obscene, discriminatory, defamatory, offensive or abusive. Offenders may not only be subject to disciplinary action of the Hospital, but also legal liability, as appropriate.

7. Email should be written in a way that only needs to be read in order to figure out what the main point is and if any kind of response is wanted or needed. Hospital staff members are advised to read "Tips to write an email" on the website of IT Support Centre.

8. Hospital staff members or offices with genuine operational need could apply for a Windows account, an email account and/ or network share access by completing an Application Form for Network/ Email Account (PPDH 1001) that available on the IT Support Centre. Hospital staff members will be asked to read the conditions mentioned therein and comply the Section E6 of the Human Resources Manual as appropriate.

INVESTIGATION ON THE USE OF HOSPITAL EMAIL ACCOUNT

9. The Comptroller (or the Chairman of the Board of Governors or Director for the case of the Comptroller' email account) reserves the right to request IT Office to get access to any Hospital staff members' email accounts for any justified reasons, including but not limited to

(a) a formal complaint about inappropriate use of the email account in question is received; **or**

(b) Hospital staff member is found sending/ receiving inappropriate messages via the Hospital email account; **or**

(c) Unauthorised entry of or attack to the email account in question is detected.

HOSPITAL EMAIL ACCOUNT ON PORTABLE ELECTRONIC DEVICES

10. If Hospital staff members have the operational needs to get access to their workstations from a remote location, or send / receive emails through their own portable electronic devices ("PED") , they should apply, with justifications, by completing the Application Form for Remote Desktop Access Connection / Using Email on Portable Electronic Devices ("PED") (PPDH 1041) for further consideration.

11. The approval would be considered based on the job duties of the concerned staff or sustain the normal operation of the service units (e.g. access to Hospital's network in a remote location during the pandemic).

APPROPRIATE USE OF EMAIL ACCOUNT ON PED

12. Security settings should be applied to the PED of the eligible Hospital staff members using their PEDs to access the Hospital email account.

13. They should safeguard their PEDs in possession at all times and it is their responsibility to ensure that PEDs are placed in a secure environment so that their PEDs and the emails stored therein are not susceptible to be stolen, copied or tampered with. They shall not leave PEDs unattended without proper security measures.

(a) Eligible Hospital staff members using their PEDs to access Hospital email account shall be held responsible for any activities performed on their PEDs;

(b) Set password for the PEDs, with reference to the password rules set out in Section E6 of Human Resources Manual of the Hospital;

(c) Never attach the PEDs to any public/ untrusted computers and/ or network;

(d) **Encrypt** the PEDs and any removable storage card installed therein (e.g. using password or fingerprint to unlock the PEDs);

(e) Set the **idle screen** lock-out to a minimum of one (1) minute.

(f) Install anti-virus security protection applications on PEDs and ensure that the virus signature file is always up-to-date, where applicable.

(g) Scan any attachment before opening.

(h) Any PEDs **MUST NOT** be installed with software or applications that would open up security threats and compromise the Hospital network.

INCIDENT REPORTING AND LOSS OF PED

14. Eligible Hospital staff members using their PEDs to access Hospital email account must report to their supervisors and IT Office immediately the missing of a PED or if there is reason to believe the PED has been lost.

DISPOSAL OF PED

15. Before disposal of any PEDs containing Hospital email account, the Eligible Hospital staff members should inform the IT Office to disconnect the email services, and remove all emails from the PEDs.

CESSATION ON THE USE OF HOSPITAL EMAIL ACCOUNT ON PED

16. On receipt of any notification of cessation of the use of Hospital email account on PED for whatever reasons, IT Office will disable the service **within two working days**.

17. Eligible Hospital staff members should clear all the emails from the PED when cessation of the use of Hospital email account.

18. The responsible operator of the IT Office shall duly complete all areas of Part V of the Application Form for Remote Access Connection / Using Email on Portable Electronic Devices (PPDH 1041).

REMOTE DESKTOP CONNECTION

19. Hospital staff members could also apply for remote desktop connection services, if needed, by completing the Application Form for Remote Access Connection / Using Email on Portable Electronic Devices (PPDH 1041) for further consideration.

20. IT Office could grant the right to Hospital's entrusted vendors to access the internal network for necessary maintenance or operations upon request. The concerned Hospital staff member requires disseminating the Guidelines on Third Party's Remote Access to Computer Systems and Network of The Prince Philip Dental Hospital to the vendor upon the access right is granted.