E6. Regulations Governing Use of Computers and Application Systems

I. Scope

1. These Regulations are applicable to **all users, including staff members and students** of the Faculty of Dentistry ("Faculty") and Prince Philip Dental Hospital ("Hospital"); the Dental House Officers of Department of Health (hereinafter called "Users"), who have to use the Hospital's computers/ application software/ Portable Electronic Storage Devices / network or connect their own computers to the Hospital network while discharging their duties or conducting training at the Hospital.

II. General Usage

2. Subject to operational needs, the Hospital will provide personal computers in the form of desktop, notebook or portable devices, or allow Users to connect their own computers or devices to the Hospital network so as to facilitate them in carrying out duties or conducting training. The Hospital computers, portable devices, application software and/ or email accounts should be used for official purposes only.

III. General Security

3. For security reasons, passwords for turning on the personal computers or for logging in any application software such as the Dental Health Information System, Accounting Systems, Procurement and Inventory System, Facility Management System, and personnel systems, as well as Hospital's email accounts, should be set up by individual Users, and be changed periodically, say on a quarterly or half-yearly basis.

4. Users should never allow any unauthorised persons to use the Hospital computers, devices, application software, network, and/or Hospital email accounts; and should never disclose their user name and/ or passwords to any other persons even if the latter are also authorised users of the computer facilities.

5. Users are also required to log off their computers and/ or application software before leaving the computers or devices in order to prevent any unauthorised persons from using the Hospital computers, email accounts and/ or application software.

6. Users should not use public/ untrusted computers and/ or network to log into the Hospital application software, network or email accounts outside the Hospital.

7. Any abnormal or suspicious activities in the Hospital computers, application software, network or emails should be reported immediately to the Hospital's Information Technology Office ("IT Office").

IV. Access to Server Rooms

8. Only staff members of the IT Office or any personnel as authorised by a System Administrator or above are allowed to enter the Main Server Room at IT Office and other Secondary Server Rooms in different areas of the Hospital. All other Users are prohibited from entering any Server Rooms without authorisation.

9. Any vendors or sub-contractors who are authorised to enter the Server Rooms must be registered at the Security Office, and escorted by a staff member of IT Office.

10. System Administrators must ensure that the keys of the Server Rooms are kept in a secure and locked location when they are not in use.

11. In the event that any Users suspect of any unauthorised access to Server Rooms or weakness in the security control of any Server Rooms (e.g. unlocked doors), they must inform the IT Office or Security Office immediately.

V. Password

12. Adoption of strong passwords is a very important aspect in the IT security. Weak passwords may compromise the entire IT network. To mitigate such risks, all Users must take appropriate steps to secure their passwords.

13. Under normal circumstances, on approval of creation of an account to log into a system or computer, Users will be given a username and an initial password, he/ she should reset to a strong password immediately as well as to change to a new strong password regularly, ideally every six months.

14. A strong password should be created as follows:

- use a minimum of eight (8) characters
- use a mix of upper case letters, lower case letters, numbers and symbols, as appropriate;
- never use sequential numbers (e.g. 12345678) or letters (e.g. abcdefgh);
- never use a dictionary word or proper name; and
- never use or include any personal information in the password, e.g. identity card or passport number, date of birth, staff or student number, etc…

15. All users are requested to protect their passwords and should

- NOT display the passwords on the monitor, desk or any open areas;
- NOT reveal or share the passwords to anyone, including colleagues or classmates;
- NOT use the function of "Remember Password" in any computers.

VI. Computers and other IT Equipment

16. Users are requested to comply with the following rules when using the Hospital computers:

(a) In general, computers owned by the Hospital should be used for work-related or training-related purposes.

(b) Users should ensure the safe custody of the computers.

(c) Hacking or seeking unauthorised access to remote or local network computers, and modifying and destruction of other persons' data are strictly prohibited.

(d) Downloading illegal copies of software, music, videos or other copyrighted materials are strictly prohibited.

(e) Spreading of immoral materials, such as pornography, violence or other offensive materials, are strictly prohibited. All Users must comply with the

Guidelines on Blocking Websites Containing Pornography, Inappropriate and Offensive Material available on the website of IT Support Centre.

(f) Dissemination of confidential information, such as patients' personal or clinical information, is strictly prohibited.

(g) Some Users may need to use internet for searching information when carrying out their duties or conducting their training. They are required to ensure that internet services are used for official purposes only.

(h) The Hospital has installed Endpoint Detection and Response (EDR) software in all Hospital computers to continuously monitors and analyzes endpoint activity to detect, investigate, and respond to threats. If the computers are attacked by viruses or when the EDR software does not function properly, the Users should report to the IT Office immediately. Users are reminded:

- **NOT** to open any attachments to the emails received from unknown sources;
- **NOT** to follow URL links from untrusted sources; and
- **NOT** to download any unauthorised software through the internet.

VII. Software

17. All Users are requested to observe and comply with the following regulations while using the Hospital computer software:

(a) The Hospital has licensed copies of computer software from several vendors. Licensed and registered copies of software programmes have been placed on computers within the Hospital and appropriate backup copies made in accordance with the licensing agreements. No other copies of these software or its documentation can be made without the express written consent of the software publisher.

(b) As far as practicable, the Hospital will provide copies of legally acquired software to meet all legitimate needs for all of its computers. The use of software obtained from *any other sources* could present security and legal threats to the Hospital. Such use **is prohibited** unless approved by the Comptroller.

(c) Software without licence, computer games or any other unauthorised software is not allowed for installation onto the Hospital computers.

(d) In some cases, the licence agreement for a particular software programme may permit an additional copy to be placed on a portable computer or home computer for business purposes. However, for control purpose, users should **not** make such additional copies of software or its documentation without the written approval of the Comptroller.

(e) **Unauthorised duplication of copyrighted software or documentation** is a violation of the law. Users who make, acquire, or use unauthorised copies of copyrighted software or documentation in the Hospital **will be subject to**

immediate disciplinary actions, including summary dismissal of employment or expulsion from study.

(f) The Hospital reserves the right to protect its reputation and its investment in computer software by enforcing internal controls to prevent the installation or use of unauthorised copies of software. These controls include:

(i) frequent and periodic assessments of software use;

(ii) announced and *unannounced* audits of Hospital computers (including notebooks); and

(iii) removal of any software found on the Hospital's property for which a valid licence or proof of licence cannot be determined.

VIII. Storage and Dissemination of Personal Data or Classified Information in Electronic Format

18. No matter how much personal data or classified information (e.g. clinical data in the Dental Health Information System) is involved and how such data or information is obtained, all users are **forbidden** to take any personal data or classified information, in any form, out of the Hospital, in particular,

(a) any employees' personal data;

(b) any students' personal data;

(c) any patients' personal data, which include identification document number such as HKID and passport number, name, date of birth, photo showing face without masking, email address, phone number, pager number, address and name of emergency contact person.

19. Should there be a genuine need to take patients' potentially sensitive data, such as X-ray film without any personal data, out of the Hospital, e.g. for making a presentation outside the Hospital or preparing course work or for research purpose, the users are required to apply effective protective measures on the electronic copies, e.g. by encrypting the electronic copy with a password.

20. Users should not send any personal data or classified information through the Internet without having assessed the security risks and adopted the necessary protective measures.

IX. Requirements under Personal Data (Privacy) Ordinance

21. In the case of personal data, users should also familiarise themselves with the provisions of the Personal Data (Privacy) Ordinance (PDPO), Cap. 486 concerning data protection. Among other things, the law requires data users to observe certain principles on the accuracy and duration of retention, use and security of personal data. Specifically, PDPO stipulates that all practicable steps shall be taken to ensure that personal data held by a data user are protected against unauthorised or accidental access, processing, erasure or other use having particular regard to:

(a) the kind of data and the harm that could result if any of those things should occur;

(b) the physical location where the data is stored;

(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;

(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and

(e) any measures taken for ensuring the secure transmission of the data.

X. Supplementary Information

22. Hospital employees and students should also refer to the following documents as uploaded on the website of IT Support Centre:

- Service Manual of the IT Office
- Guidelines on the Use of Hospital Windows Accounts, Email Accounts, Access through Personal Electronic Devices and Remote Desktop Connection
- 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 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

as well as the following kits:

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

XI. Enquiries

23. Users may consult the IT Office for technical support if necessary.

24. Users may also visit Hong Kong Computer Emergency Response Team Coordination Centre's website (www.hkcert.org) for the most up-to-date computer security measures and advice.