NUHS
National University Health System

# LETTER OF UNDERTAKING

I hereby undertake that at any time **before, during and after** my employment/ posting/ appointment/ training/ attachment with the National University Hospital (the "Hospital") and the National University Health System ("NUHS"), that:

1. I shall strictly observe the confidentiality of Hospital and NUHS proprietary or confidential information including patient information and personal data contained in any medium including in hardcopy or electronic form ("**Information**").

2. My attention has been drawn in particular to the following:
   a. the Personal Data Protection Act 2012 (Act 26 of 2012);
   b. the Computer Misuse and Cybersecurity Act (Cap. 50A);
   c. the Official Secrets Act (Cap.213) and in particular to section 5;
   d. the Income Tax Act (Cap. 134) and in particular to sections 6(1), (2) and (3); and
   e. Infectious Diseases Act (Cap. 137).

   My attention has also been drawn to the relevant Hospital and/or NUHS policies concerning confidentiality and data protection.

3. I shall not divulge any Information to any unauthorised person.

4. I shall not access, copy, reproduce or use any Information for any unauthorised purpose.

5. I shall promptly return all Information when I leave the employment/ posting/ appointment/ training/ attachment of the Hospital and/or NUHS. This includes all hardcopy materials, electronic materials, softcopies and templates. I acknowledge that all or some of the Information is intellectual property that belongs to the Hospital, NUHS, or some other party.

6. I shall not communicate to external parties (including but not limited to business contacts, media, competitors, external authorities, etc.) matters concerning my work or any Information (whether conveyed formally or otherwise) without prior approval from the Hospital and/or NUHS.

7. I will be deemed to be in breach of Hospital and/or NUHS policies and the terms of my employment/ posting/ appointment/ training/ attachment, concerning confidentiality and the protection of patient information and personal data, and hence liable to disciplinary or other action, if I access any patient information with respect to patients not directly under my care or purview, or if I access any personal data without authority.

8. If I am given access to the hospital systems which has access to patient information, it is my duty to ensure that I log off my account after use. Failure to do so would result in breach of Hospital and/or NUHS policies, and I may be liable to disciplinary action.

9. I understand that the Hospital and NUHS view any breach of any confidential patient information or personal data very seriously and that the Hospital and/or NUHS reserve the right to undertake termination and legal action in the event of any such breach or similar offences thereto.

10. I hereby agree to indemnify the Hospital and NUHS on a full indemnity basis, against all costs, fees and expenses (including costs of the Hospital's and/or NUHS' solicitors and other professionals, where applicable and whether or not legal, arbitration or other proceedings are instituted) incurred by the Hospital and/or NUHS in the event of a breach of any of the provisions herein, whether directly or indirectly by any act, omission, neglect or other default on my part.

11. I further understand and agree that any breach or neglect of the terms herein may render me liable to prosecution under Singapore statutes and the relevant subsidiary legislation, including but not limited to the Personal Data Protection Act, the Computer Misuse and Cybersecurity Act, the Official Secrets Act, the Income Tax Act and the Infectious Diseases Act.

12. I consent to the collection, use, disclosure and processing by the Hospital and/or NUHS of all personal data that I provide to the Hospital and/or NUHS for the purposes of my *employment / posting / appointment / attachment with the Hospital and/or NUHS.

**Signed By:**

| | | |
|---|---|---|
| Employee's Full Name in Blocks | Signature of Employee | NRIC / Passport No. |
| Designation | Department | Date |

# ACCEPTABLE USE POLICY OF IT EQUIPMENT & SYSTEM ACCESS

This Acceptable Use Policy (AUP) communicates in clear language how IT systems and network resources are to be used at National University Health System (NUHS) so that computing is safe, secure and reliable.

**1. Responsibilities for Security and Confidentiality**

1.1 All healthcare IT users must guard the confidentiality of NUHS data (including patient information, medical records, staff information and any business matters).

1.2 Access to healthcare IT systems and confidential information is strictly for work and on a "need-to-know" basis.

1.3 You shall only access IT systems which you have been authorized to use, and shall not attempt to exceed the access levels given to you.

**2. User Accounts and Passwords**

2.1 You are responsible for your user account. You must guard your account and password. Never share or allow others to use your account.

2.2 You are accountable for all activities performed using your account in NUHS IT systems.

**3. Securing Information and Equipment**

3.1 Secure your devices against theft at all times. Always protect your laptop with a cable lock. Store your laptop in a locked cabinet after office hours. Keep your mobile phones, thumb drives and portable hard disks under lock and key when not in use.

3.2 All confidential information must be protected. Electronic documents with confidential information must be password protected.

3.3 You must return all institution-issued devices no later than your last working day with NUHS.

**4. Internet, Intranet and Corporate Network**

4.1 Do not connect your personal devices to the corporate network, computers or equipment. **Only** institution-issued IT computing equipment and mobile devices (such as PCs, laptops, iPads, PDAs, thumb drives and external hard disks) can be used for official work.

4.2 Sharing work-related confidential information (e.g. patient information or confidential corporate information) on social network sites (e.g. Twitter, LinkedIn, Facebook and WhatsApp) is **not** allowed.

4.3 Using cloud storage services (e.g. Google Drive, Dropbox etc.) to store classified (restricted/confidential/secret) documents or information is **not** allowed.

4.4 Always log off from the system when you are not using your devices.

**5. Corporate Email Usage**

5.1 Your NUHS email account is strictly for official work and is not for personal matters.

5.2 Personal email accounts cannot be used for any NUHS work.

5.3 You must never forward your NUHS emails to your personal email account.

**6. Obligation to Report**

6.1 Report to NUHS IT Helpdesk in the event of:

- a IT security problem or suspected malicious emails;
- any breach or suspected breach of the terms governing the use of IT systems;
- any misuse or abuse of IT systems; and
- loss of IT equipment.

**7. Rights to Audit and Monitor Use**

7.1 NUHS reserves the rights to audit and actively monitor all your activities on its IT systems, to ensure their proper and secure use. You will be asked to account for any unauthorized access identified.

**8. Penalties for Breach**

8.1 You shall be subjected to potential liability and disciplinary actions for any breach of the terms of use.

---

I hereby undertake that at any time before, during and after my employment/ posting/ appointment/ attachment with entities of the National University Health System ("NUHS") that I shall observe the AUP clauses mentioned above.

| **Signed By:** | | |
|---|---|---|
| Full Name in Blocks | Signature | Employee No./NRIC |
| Designation | Department | Date |