

Instruction to Students on Accessing Online Teaching

This document is divided into 5 sections:

1. Guiding Principles
2. Training
3. Accessing Sessions Facilitated by College
4. Accessing Sessions Facilitated by Trusts and Primary Care Providers
5. Consequences of Failure to Follow this Instruction

1. Guiding Principles

- The General Medical Council (GMC) has published guidance on the standards of behaviour expected of medical students in this guide: [‘Achieving Good Medical Practise: Guidance for Students’](#)
- In the section on “Maintaining patient confidentiality”, that guidance states:
 - *“All patients have a right to expect that their doctors will hold information about them in confidence.”*
 - *“Many improper disclosures are unintentional. You must not share identifiable information about a patient where you can be overheard, such as in a public place or on social media, or include it in any work or logbooks you submit.”*
 - *“You must also follow any policies of your medical school, university or placement provider to make sure personal information is stored and disposed of securely.”*
- The ongoing challenges presented Covid-19 pandemic mean some patient contact will now be virtual
- In these challenging circumstances, Imperial College School of Medicine (ICSM) expects its students to observe the same high standards of personal and professional conduct observed under normal circumstances

2. Training

- Students are reminded they should complete data protection awareness training to enable them to comply with [College Data Protection Policy](#)
- As part of your programme of study, students must complete [ELFH data protection training](#)
 - This training is undertaken by all NHS healthcare professionals
 - This training is accepted by College as equivalent to College data protection training
 - Year 2 and 4 students should have successfully completed this training
 - Year 1, 3, 5 and 6 students are required to successfully complete this training
 - Faculty Education Office (FEO) administrators will facilitate this training as part of the MBBS programme of study
- Additional information and guidance regarding data protection is available on the [College website](#)

3. Accessing Sessions Facilitated by College

- Online sessions that include identifiable patient data must be delivered using the College’s version of Microsoft Teams
- Students should only access these sessions using their @imperial.ac.uk email address

- To avoid improper disclosures, unintentional or otherwise, ICSM stipulates the following:
 - Students must ensure any personal computers and devices – laptops, tablets, phones – are secure before accessing identifiable patient data:
 - Imperial College Information and Communication Technology (ICT) offer free security checks to all Imperial students
 - Security checks can be raised via an ASK request or phone call:
 - <https://www.imperial.ac.uk/admin-services/ict/contact-ict-service-desk/>
 - For further guidance on how to keep be secure, ICT has guidance on security available online:
 - <https://www.imperial.ac.uk/admin-services/ict/self-service/be-secure/>
 - Students must ensure their internet connection is private and secure
 - Public networks must not be used - airports, libraries, hospitals, coffee shops, restaurants, for example
 - Private networks may be used – Wi-Fi networks in your home, for example – provided they are secure
 - The Information Commissioner’s Office (ICO) has provided advice on Wi-Fi security:
 - <https://ico.org.uk/your-data-matters/online/wifi-security/>
 - Students must not access identifiable information about a patient where they can be overheard or interrupted, such as:
 - a public place – café, restaurant, shop, park etc.
 - external or outdoor spaces
 - a shared area or communal area of a private residence – lounge, stairway – where they are likely to be disturbed or others may be present
 - Students are expected to wear headphones to listen to content wherever possible
 - Private recordings of virtual clinical are forbidden under all circumstances
 - Recordings will be made available by ICSM where appropriate
 - Identifiable patient data must not be disclosed or discussed on social media or by private means with a third party
 - All personal notes in all formats related to sessions must not include identifiable patient data
 - Where in doubt, students must exercise extreme caution and discretion in handling identifiable patient data
 - Students must raise concerns in a confidential, non-judgemental way about fellow students, clinicians, lecturers or staff who fail to observe the rules outlined above or who behave in a manner likely to result in an improper disclosure

4. Accessing Sessions Facilitated by Trusts and Primary Care Providers

- Online sessions that include identifiable patient data may be delivered by trusts or primary care
- In these circumstances, the trust or primary care provider control the data made available to ICSM students
- ICSM students are expected to abide by the local trust or primary care provider regarding information security and data protection
- Nevertheless, the guiding principles outlined in the first section of this document still apply
- In most circumstances, students will access the information using their @NHS.net email address, but they should always abide by local policies.
- To avoid improper disclosures, unintentional or otherwise, ICSM advises the following:

- Students should access these sessions on trust or primary care provider premises (except for Multidisciplinary Team Meetings (MDT))
 - Students attending online Multidisciplinary Team Meetings (MDT) must use headphones and ensure they are in a private space with a private and secure internet connection
- When on trust or primary care provider premises, students must not access identifiable information about a patient where they can be overheard or interrupted
- Students are expected to wear headphones to listen to content wherever possible
- Students must ensure they use the relevant NHS secure internet connection and not use any local free or publicly available Wifi
- Students should use trust or primary care provider hardware or devices wherever practicable
- Students should ensure any personal computers and devices – laptops, tablets, phones – are secure before accessing identifiable patient data
- Private recordings are expressly forbidden under all circumstances
- Identifiable patient data must not be disclosed or discussed on social media or by private means with a third party
- All personal notes related to sessions must not include identifiable patient data
- Where in doubt, students must exercise extreme caution and discretion in handling identifiable patient data
- Students must raise concerns in a confidential, non-judgemental way about fellow students, clinicians, lecturers or staff who fail to observe the rules outlined above or who behave in a manner likely to result in an improper disclosure
- Accessing Sessions Facilitated by Trusts and Primary Care Providers for those students self-isolating due to COVID-19:
 - If a student is required to self-isolate as a result of COVID-19 (either due to becoming symptomatic themselves or due exposure to a contact), they may be able to access clinical sessions remotely from their own home, **with the explicit agreement of the placement provider**. In this situation, **the student will either observe their clinical supervisor consulting with patients or the student may consult directly with patients with appropriate clinical supervision for each patient contact**. Students accessing clinical sessions in this way are reminded that the requirements outlined in the previous sections of this document above continue to apply.

5. Consequences of Failure to Follow this Instruction

- Failure to observe any of the rules outlined above will be considered a breach of confidentiality and therefore failure to demonstrate good medical practice that could result in the initiation of Fitness to Practise (FTP) proceedings
- Failure to observe any of the rules outlined above may also result in College disciplinary proceedings