COVID-19 – Working from Home

Privacy and Data Security Guide

While working from home, all staff must conduct University business with the same standards of privacy, confidentiality and security that ordinarily apply. Greater risks arise from mass operations of the University now being conducted through online platforms, and each individual staff member must act cautiously in undertaking their usual duties which involve University information that is:

- commercially sensitive or otherwise confidential, or
- contains personal information (of students, staff, research participants, donors, alumni, prospective students or community members).

'Personal information' in this Guide refers to information by which an individual is reasonably identifiable.[1] This includes contact details, photos and videos. For example, video-recorded meetings and invigilators for online exams collect personal information in the form of a person's image.

By following this Guide, you will be implementing practices to meet the University's obligations under privacy laws and protect University information. This Guide covers privacy basics, virtual meeting requirements and safeguards for access, use, storage, transfer and disclosure of University information.

PRIVACY BASICS – legal must do's

- If you are collecting personal information from an individual or group of individuals, you need to have their informed and voluntary consent. Individual(s) must be advised of how their personal information will be used.
- You must have appropriate safeguards to protect personal information against loss, unauthorised access, misuse or unauthorised modification or disclosure. UNSW staff must follow the requirements of the Data Classification Standard and use platform/software that is sufficiently secure.

VIRTUAL MEETINGS AND VIRTUAL TEACHING

Staff should use University-approved platforms for web conferencing and conducting virtual teaching. It is important staff select the most appropriate platform and apply the necessary security settings to protect University information and ensure it is secure.

[1] the information actually identifies or could reasonably be used to identify the individual

The collaboration platform 'Teams' (Microsoft Office 365) is known to be a secure platform with strong default settings to protect access and storage. Teams functionality includes basic calls, meetings up to 350 attendees and live events up to 10,000 attendees and training is available on the UNSW IT website.

The web conferencing tool 'Zoom' has meeting functionality. Staff who are responsible for arranging the meeting should adjust security settings to limit access and avoid inappropriate use, including setting meeting passwords, using the 'waiting room' function and disabling file transfers. Staff should follow UNSW IT's advice on use of Zoom.

> ***Ensure the appropriate security for any meeting that will discuss or distribute information that is commercially sensitive or otherwise confidential and/or that contains personal information.***

Recording (including audio, audio and video recording, screen capture and photographing)

There must be a genuine business need to record any discussion. In addition, recordings must comply with privacy law obligations, including obtaining the necessary consent and safeguarding access and storage.

> ***Follow the UNSW Recording Practices (Privacy Requirements) which provides you with instructions and proforma wording to enable UNSW to meet its privacy law obligations.***

Meetings between UNSW staff and/or third parties

Meetings between UNSW colleagues must not be recorded unless there is a genuine business need to record, and staff should ask themselves – *would I record this meeting if it was being conducting face to face?*

The meeting should not be recorded unless all participants provide their consent to the meeting being recorded. See UNSW Recording Practices for gaining consent.

UNSW staff and students (lectures, tutorials and meetings)

Recording for purposes other than educational instruction is prohibited. The same principles apply to the conduct of virtual contact as those in a face to face setting.

Lectures

UNSW has had lecture recording facilities in place for over ten years and staff do not need to undertake any additional steps to meet privacy requirements if they continue to use these well-established facilities. See the UNSW staff sites for Teaching Remotely Sharepoint Site and UNSW Teaching Gateway.

Tutorials & Meetings

Tutorials and meetings must not be recorded unless there is a genuine need to do so and all students participating have provided their consent in advance of the tutorial/meeting to be recorded. See UNSW Recording Practices for gaining consent.

PRIVACY & DATA SECURITY - PRACTICES FOR SAFEGUARDING UNIVERSITY DATA

General Safeguards

Only use UNSW devices or UNSW-approved 'Bring your own devices' (BYOD) to conduct your work duties and do not allow access to your work devices to non-UNSW employees.

Ensure your work devices are up-to-date with all UNSW systems and software updates. Do not install unauthorised software on your work devices and ensure all UNSW systems and software are up-to-date to protect against threats.

Be alert to phishing and malicious attacks. Be extremely cautious about emails from unknown sources and opening links in any email which is not clearly from a known or genuine source. Note that malicious emails may adopt UNSW's general 'look and feel' – always closely check the sender email address and other details if the email is from an unknown person.

Report any suspicious communications you receive via ITU Service Centre

Access & Use Safeguards

Setting devices to lock automatically for periods of no-use. When sharing space in your homes with non-UNSW employees, you should always ensure your devices are locked with password protection when not in use.

Minimum Necessary Rule

Only use the specific information needed to complete your work duties. You should only access the information required to complete the specific task you are working on, especially if the information contains personal information, confidential or sensitive material.

Avoid Univeristy information being in locations which non-UNSW staff may be able to access. Avoid commercially sensitive, confidential and personal information being printed, or saved on personal devices or storage devices without appropriate password protection, unless the reason to do so outweighs the risk and you have taken all appropriate precautions to avoid unauthorised use and access.

Transmission & Storage Safeguards

UNSW ✓

Only use UNSW approved systems and software to transfer, share or store University information. UNSW has approved systems and software that meet the security needs of the University. All commercially sensitive, confidential and personal information is regarded as 'Sensitive' or 'Highly sensitive' and you must only use the appropriate system or software requisite to the sensitivity. OneDrive is considered secure for sharing and storing documents.

Never use unsecured, non-UNSW systems and software (e.g. Facebook, Dropbox etc) to transfer, share or store University information.

Have further questions or need specific advice?

Specific confidentiality and privacy concerns arise in relation to the use of digital communication and meeting platforms and software. For further advice or queries, please contact:

Privacy
privacy@unsw.edu.au

For advice on:

- Privacy clauses in contracts
- Privacy requirements for recordings
- Privacy generally
- COVID tracing and what personal and health information can be shared and disclosed

To make a formal privacy complaint

Legal
legaloffice@unsw.edu.au

For advice on:

- Confidentiality
- Legal issues arising from COVID

IT
www.myit.unsw.edu.au/working-and-studying-remotely

For advice on:

- Data security and technical requirements
- Cybersecurity

For training on:

- OneDrive
- Teams/Zoom

UNSW RECORDING PRACTICES - PRIVACY REQUIREMENTS

Practices to Implement

UNSW Staff Meetings	Lectures	Tutorials and Staff-Student Meetings
These are not recorded as a matter of standard business and consent must be obtained. Consent must be voluntary and participants must not be forced to agree to the recording. ***Recording must not occur unless you have the consent of all participants.***	*Lectures are recorded as a matter of standard business and UNSW has incorporated processes to meet its requirements.*	*Tutorials and staff-student meetings are not recorded as a matter of standard business and consent must be obtained. Consent must be voluntary and participants must not be forced to agree to the recording.* ***Recording must not occur unless you have the consent of all participants.***
1. ***Genuine Business Need*** – only propose recording the meeting if there is a genuine business need and that need would not otherwise be met (e.g. through note-taking). 2. ***Written Notice*** – in the meeting invitation provide clear notice that you intend that the meeting will be recorded and the purpose of the recording. TIP: Use the meeting template on the next page. 3. ***Verbal notice –*** in addition, you must inform all attendees that the meeting will be recorded and the type of recording (audio or audio and video). This should be done: (a) at the start of the meeting (b) when an individual joins the meeting who was not present at to hear the notice at the start of the meeting 4. ***Do not force consent*** – you must not proceed with the recording unless all participants have consented to being recorded 5. ***Allow participants to adjust settings*** - allow time for those individuals who consent to adjust their personal settings (e.g. turn off video, blur background etc) to do so prior to the recording being initiated. 6. ***Control the recording*** – You should monitor and manage the recording. Be sure to prevent or stop the recording if it is: - inappropriately initatied by someone other than yourself - captures inappropriate behaviour or conduct	***Follow existing guidelines*** – Staff should use established facilities arranged for running and recording lectures, e.g. Echo360 Universal Capture. There is guidance on setting up recording and general rules available on the teaching staff sites: Teaching Remotely Sharepoint Site and UNSW Teaching Gateway Site. It is important staff holding the lecture ensure they control the recording and do not capture any unintended or inappropriate material.	1. ***Genuine Business Need*** – only propose recording the meeting if there is a genuine business need and that need would not otherwise be met. 2. ***Written Notice*** - provide advance written notice that you intend to record the tutorial(s) or meeting. This notice can be given in the meeting invitation or in a separate communication. Inform all participants/students that the recording will only occur if all participants/students provide consent, the tutorial/meeting you intend it to be recorded, explain the type of recording (audio or audio and video) and the purpose of the recording. Ask students to provide a response stating their consent or declining consent. 3. ***Verbal Notice –*** in addition to the advance written notice of your intention to record the tutorial/meeting, confirm this verbally at the start of the tutorial/meeting (this ensures that everyone present is aware – some participants may have missed the written communication). 4. ***Do not force consent*** – you must not proceed with the recording unless all participants have consented. to being recorded 5. ***Allow students to adjust settings -*** You should advise students of the options available to them to adjust video settings and provide time do so prior to the recording being initiated (e.g. turn off video, background with blur etc). 6. ***Control the recording*** – You should monitor and manage the recording. Be sure to prevent or stop the recording if it is: - inappropriately initatied by someone other than yourself e.g. if a student starts the recording function - captures inappropriate behaviour or conduct

Template – Recording - Meeting Request

Copy and paste the following:

- This meeting will be recorded -

[Your meeting message goes here.]

[Signature]

RECORDING DETAILS

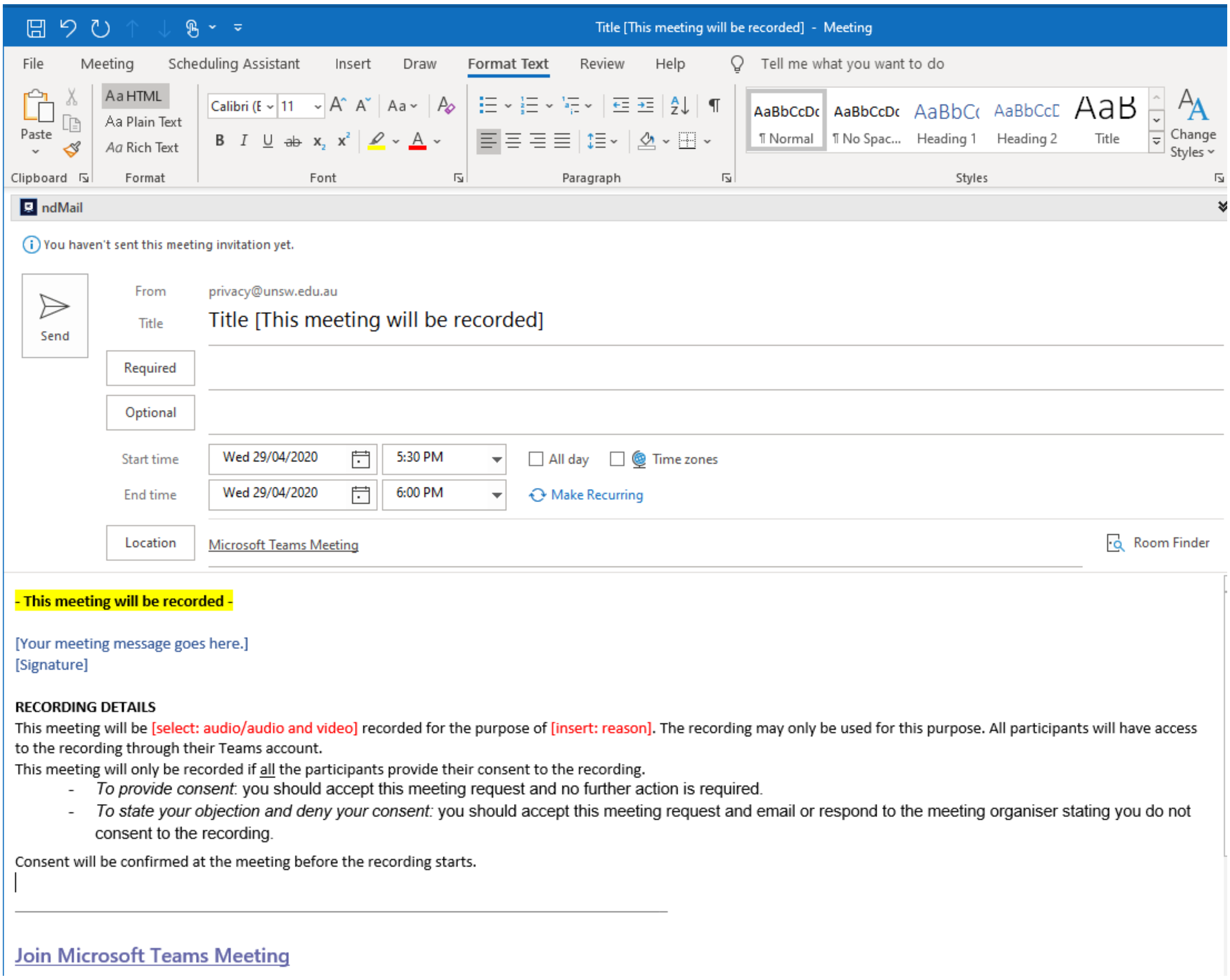
This meeting will be [select: audio/audio and video] recorded for the purpose of [insert: reason]. The recording may only be used for this purpose. All participants will have access to the recording through their Teams account.

This meeting will only be recorded if all the participants provide their consent to the recording.

- *To provide consent*: you should accept this meeting request and no further action is required.
- *To state your objection and deny consent*: you should accept this meeting request and email or respond to the meeting organiser stating you do not consent to the recording.

Consent will be confirmed at the meeting before the recording starts.

Sample



You haven't sent this meeting invitation yet.

From: privacy@unsw.edu.au

Title: Title [This meeting will be recorded]

Start time: Wed 29/04/2020 5:30 PM

End time: Wed 29/04/2020 6:00 PM

Location: Microsoft Teams Meeting

- This meeting will be recorded -

[Your meeting message goes here.]
[Signature]

RECORDING DETAILS

This meeting will be [select: audio/audio and video] recorded for the purpose of [insert: reason]. The recording may only be used for this purpose. All participants will have access to the recording through their Teams account.

This meeting will only be recorded if all the participants provide their consent to the recording.

- *To provide consent*: you should accept this meeting request and no further action is required.
- *To state your objection and deny your consent*: you should accept this meeting request and email or respond to the meeting organiser stating you do not consent to the recording.

Consent will be confirmed at the meeting before the recording starts.

Join Microsoft Teams Meeting