Zoom & Data Protection: Guidance for DCU Staff

This document contains guidance for DCU staff and researchers under the following headings:

Important note: ***This document is not definitive, and does not constitute legal advice.***

Use this document as a guide, only, to understand your options while using Zoom.

Where necessary, please refer to specific guidance below on Teaching and Research contexts, as these may require deviation from the following General Guidance.

1. General Guidance

1.1 Normal Data Protection rules apply

Data Protection and data security

Each Zoom user has a responsibility to ensure they understand and comply with basic Data Protection and data security requirements.

The majority of Data protection Breaches occur due to human error, rather than as a result of a technological fault. Therefore, users should be familiar with data protection rules and the functionalities of Zoom before use, and be mindful of these requirements while using Zoom.

Familiarise yourself with your Data Protection obligations

The DCU Data Protection Unit (DPU) recommends that all DCU staff and researchers complete the DPU's online training module. This is a short introductory course, setting out key data protection principles, concepts and requirements under GDPR.

- **This module can be accessed at the following link: Introduction to GDPR**

Familiarise yourself with Zoom

All DCU staff and researchers are strongly encouraged to familiarise themselves with the features, configurations and settings within Zoom.

- **Online tutorials can be accessed at the following link: Zoom online tutorials**
- **Ensure you check for updates so that you have the most recent version of Zoom**

Specific queries

For specific queries concerning data protection, please contact the Data Protection Unit (DPU).
For specific queries concerning Zoom, please contact the Teaching Enhancement Unit (TEU).
Other technical issues may be raised with Information Systems Services (ISS).

These units can be contacted via the following links:

- Data Protection Unit
- Teaching Enhancement Unit
- Information Systems Services

Personal Data and GDPR obligations

- **Personal data** means "any information relating to an identified or identifiable person," whether directly or indirectly. This includes written information and records, video images and still images, Student ID, user names and user nicknames.
- When using Zoom, DCU is regarded as a 'Data Controller'. **Accordingly, all DCU staff as employees of the Data Controller, must abide by data protection rules and obligations under GDPR when using Zoom.**
- Zoom is a 'Data Processor' where a user, such as DCU, uses it services. Zoom provides a service to and for DCU, and must itself comply with GDPR.

1.2 Security & Privacy

Configuring settings

For security reasons, many Zoom settings are configured at a DCU corporate level, and cannot be tailored to individual settings. These include:

- **Accessing a Zoom meeting**
    - Participants are not allowed join before the Host.
    - Unique meeting IDs are required for each scheduled or instant meeting (rather than using a Personal Meeting ID (PMID).
    - Participants cannot re-join a meeting if the Host has removed them.
    - Guests from outside DCU are identified.
    - Telephone numbers masked.
- **Recordings & Transcripts**
    - Participants cannot save a transcript of the call.
    - Meetings are not recorded automatically: only the Host may do this and access these recordings.
    - Recording to local files is not allowed (cloud only).
- **Other security measures**
    - Files cannot be transferred via chat.

Other Zoom settings are accessed through the Zoom online portal for DCU. These can be configured as a default for all your meetings, or individually per meeting.

- **Configure your meeting settings here.**
- **Settings for individual meetings and your personal meeting room here.**

A recent security feature added to Zoom's meeting controls is a **Security Icon** in your meeting controls, which simplifies how meeting hosts can quickly find and enable many of Zoom's in-meeting security features.

Visible only to Hosts and co-Hosts, the Security Icon provides easy access to several existing Zoom security features so you can more easily protect your meetings. Read more here.

Zoom instant messaging / chat

- **Avoid** using Zoom's instant messaging/chat feature for written communications while using Zoom. Instead, use alternative, reliable and secure communication methods such as your DCU Gmail account.
- Please be mindful that such communications constitute work-related records and are subject to the normal rules applicable under Data Protection and Freedom of Information legislation, as well as DCU's own policies (e.g. HR and IT).
- Discretion is advised and such communications should not be considered private.
    - **For example**, if participants of a Zoom call use the chat feature to discuss another participant's contribution, including making personal comments about the individual, the full transcript of this chat can and will be provided to that individual in the event that they request a copy in accordance with their data protection rights under GPDR.

1.2.1 Tips for Zoom meeting 'Hosts'

Setting up your Zoom meeting

- When setting up your Zoom meeting, **do not share links** publicly, including on social media. To do so would make your event extremely public, meaning anyone with the link could join your meeting. A known issue is for Zoom meetings to be interrupted by gate-crashers (aka '**Zoombombing**').
- **Familiarise yourself** with Zoom's settings and features, including by completing Zoom online tutorials, so you understand how to protect your virtual space when you need to.
- **Use a meeting password**, and ensure that you **change passwords for each meeting**, including for recurring meetings.
- **Use a unique link for your meeting** – do not use a link for your general meeting room.
- **Require registration**, and only circulate the meeting link approx. 30 minutes beforehand.
- **Use the 'Waiting Room' feature**, and only let in people who are registered for the call.

Audio, video, chat and screen sharing settings

- Change **audio** settings so that only the Host can control the audio.
- Set the **chat** setting, so that participants can only message the Host.

- Set **screen sharing** to “Host only”. (The default setting on Zoom allows all participants to share what's on their screens with the group, replacing the host's own camera feed, so ensure you change this setting immediately.) Alternatively, set calls/meetings audio-only.
- Disable “Join before host”.
- Enable encryption. This prevents people on your network or wifi from snooping on a meeting. More on Encryption.
- Begin the call with all video and audio muted.
- Avoid using your Personal Meeting ID (PMI) to host public events. Your PMI is basically one continuous meeting and you don’t want strangers crashing your virtual space after the party’s over. Learn about meeting IDs and how to generate a random meeting ID in this video tutorial (at the 0:27 mark).

During the Zoom meeting

Manage attendees: Hosts and co-hosts can manage attendees in the following ways.

- Request that a participant unmutes
- Stop a participant's video
- Rename a participant
- Put a participant on hold if enabled
- Lock the meeting to prevent anyone new from joining
- Place participants in waiting room or admit/remove participants from the waiting room.
- More on managing participants in a meeting.

Add a co-host: Controlling a meeting while giving a presentation or talk might be challenging. You can assign a co-host to perform most host duties for you while you lead the meeting. More on Adding a Co-Host

1.2.2 Tips for Zoom users

- **Do not share Zoom meeting invites** you have received from a meeting host.
- **Keep your apps updated:** In line with recommended good practice from ISS, you should keep all apps up to date, and this applies equally to Zoom.
- If you use the Zoom iOS app, **ensure it has been updated** to the latest version to ensure that their personal data is not automatically shared with Facebook Inc.
- **Change meeting passwords regularly.**

1.3 Data Protection incidents / breaches: what to do?

Do not panic.

Notify the DCU Data Protection Unit (DPU) immediately if you become aware of a potential data protection incident or breach, or if you suspect that one may have occurred: **data.protection@dcu.ie**.

In the event of a data protection incident or breach occurring:

- Ensure that you retain any and all records involved, until you have received DPU advice.
- Provide as much detailed information to the DPU as possible, in order to assist the DPU in investigating and managing the incident. This can be done by completing the Data Incident / Breach Report referenced below.
- The DPU may seek further information or clarification, and may provide you with recommendations to mitigate against the risk of a similar incident occurring again.

Guidance on reporting Data Protection incidents or breaches is available on the DPU website:

- **Data Breach Reporting Procedure - Public Guide**
- **Data Breach Reporting Procedure - Staff Guide** (Staff Access Only)
- **Data Incident / Breach Report** (Staff Access Only)

Where an incident occurs, the DPU's priority is **containment** of the incident and **mitigation** of any risks which have been identified as a result.

Your assistance is crucial in achieving these, and the DPU will support you and your colleagues in responding to any such incidents.

2. Guidance for Teaching

At the beginning of a class

- **Participants should be informed of their rights and obligations in respect of data protection/privacy at the outset of each online class.** This may be by way of introduction to the class and/or setting 'ground rules,' for example, to include a point which clearly relates to data protection, and which is preferably done using accurate but plain English.

Zoom Classroom

- In the teaching context, teaching staff should set up Zoom Classrooms on their Loop module pages and within those, schedule teaching sessions ('meetings') for their students. This ensures students have a central location in which to access teaching sessions and cloud recordings thereof. **This resource explains how to set up a Zoom Classroom on Loop**.

Breakout Rooms feature

- The data protection rules which apply to the main Zoom Classroom equally apply within the Breakout Rooms.
- Teaching staff should remind students that data protection rules apply, before the breakout session begins.

Chat/Messaging and Whiteboard/Annotation features

- In the teaching context, it may be deemed appropriate by the teaching staff to use the chat/messaging and whiteboard/annotation features as part of pedagogical methodologies, tools and techniques used to engage students.
- If so, staff must consider on a case-by-case basis whether this is appropriate, taking into account factors such as class size, topic under discussion, degree of sensitivity of the topic.
- Any personal information processed using Zoom, including information exchanged using these features, is subject to the rules of Data Protection.
- This therefore entails a level of risk which the teaching staff member themselves must assess and mitigate.
- Where such features are used, teaching staff must remind students that these facilities must be used appropriately, that data protection rules apply, and not to share personal data.

Waiting Room feature

- Where large classes are involved it may not be practicable to use the '**Waiting Room**' feature as a security measure, since it will require approving each participant one-by-one.

Screen sharing

- Where **screen sharing** by students is used as part of the teaching process (for example, giving presentations to the class), the teaching staff member may wish to adjust their Zoom controls to facilitate this. Accordingly, teaching staff should familiarise themselves with the screen sharing feature in Zoom, and understand how to switch it on and off as appropriate.

3. Guidance for Researchers

3.1 Online interviews

At the time of writing, Zoom has updated its encryption standards to improve security and ensure end-to-end encryption. Therefore, in the context of research involving human participants, **subject to specific safeguards put in place by the researcher, Zoom may now be used for interviews with human participants**, including where especially sensitive Personal Data and/or Special Categories of Personal Data are involved.

While using Zoom as part of their research, **researchers should only use the DCU licenced version of Zoom**. Researchers must ensure that they **use Zoom in a manner which is compliant with data protection requirements**, and any other legal or regulatory requirements.

The DCU Data Protection Unit (DPU) recommends that all DCU staff and researchers complete the DPU's **online Data Protection training module**. This is a short introductory course, setting out key data protection principles, concepts and requirements under GDPR.

- **This module can be accessed at the following link: Introduction to GDPR**

Zoom should only be used when specific safeguards have been implemented to ensure that:

- The appropriate Zoom security and privacy settings are activated; **and**
- Interviewees have been fully informed by the researcher of:
    - How and why they intend to use Zoom as part of the research project;
    - What will happen to the information produced as a result of the Zoom interview (e.g. any recordings, notes, transcripts, etc.);
    - How long any such information will be kept and the reasons for keeping it; and
    - How the information will be destroyed at the end of the retention period.
- Interviewees should be given the opportunity in advance to consider whether they wish to participate in the Zoom interview; **and**
- Interviewees must be given the opportunity to decline or later withdraw from the interview process.
- Interviewees must in advance be informed of their data protection rights, including: the right of access to personal data relating to them, and the right to object to the processing of personal data relating to them.

Please note that the following platforms should not be used, as they do not have end-to-end encryption and are therefore not considered to be secure:
Skype, WhatsApp, Facebook Messenger, Jitsi, Houseparty.

3.2 Consent

Under GDPR, **consent** means:

> "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

The phrase "**or by a clear affirmative action**" means that a signature is not necessarily required in order to confirm consent. Consent could be given, for example, by way of email – so long as the researcher can be certain that the email has come from the individual (the 'Data Subject') themselves, and not from any other person.

3.2.1 Consent and conducting online interviews

If the research participant has not yet provided consent

The standard consent plus information regarding the use of the online video/chat tool should be offered when seeking consent.

If the research participant has already provided consent

An addendum to this should be provided regarding the use of the online video/chat tool should be offered. This will ensure that the participant fully understands how their information is being processed, before deciding whether or not to consent.

The research participant should also be offered the opportunity to ask questions at this stage, before deciding whether or not to consent.

3.2.2 Research and children: Consent and assent

Any person under the age of 18 is a child. This applies in the context of both data protection law and research ethics.

Where a research participant is a child, the researcher must obtain **consent** from the holder of parental responsibility in respect of the child. Separately, the researcher must also obtain **assent** from the child participant themselves.

Consent: The consent obtained from the holder of parental responsibility in respect of the child is the same as described at 3.2 above, and must meet the requirements set out under GDPR.

Assent: Broadly put, assent is the agreement of someone who is unable to give legal consent to participate in the activity. The existing rules around assent continue to apply, however, the method by which assent is obtained may need to be adapted where communication is by electronic or digital means only.

Specific queries

For specific data protection queries, please contact the Data Protection Unit (DPU) **here**.

For specific research ethics queries, please contact the Research Ethics Committee (REC) **here**.

End.

Document Version Control		
Document Name	Zoom & Data Protection Guide for DCU Staff	
Version Reference	V2.0	
Document Owner	Data Protection Unit	
Approved by	Data Protection Officer	
Date	30 June 2020	