Recommendations on assessment in the context of the exceptional situation of distance teaching motivated by COVID-19

Until the competent administrations and, where applicable, the UPC's governing bodies do not adopt framework regulations regarding teaching and assessment procedures in the current context of distance teaching, we issue a few recommendations, which are detailed below. These recommendations comply with the provisions of the document *ICT Security and Personal Data Protection Criteria in Class and/or Remote Assessment* in the framework of personal data protection laws (the GDPR and the LOPDGDD).

This document is divided into four sections:
A. General recommendations for distance learning

B. Specific recommendations for distance assessment

C. ICT recommendations

D. Frequently asked questions and additional considerations

A. General recommendations for distance learning

In the case of distance learning sessions, as well as in any technical and organisational measures taken, the following general instructions regarding the processing of personal data with the tool used must be kept in mind:

1) It is recommended that the computer tools that the UPC makes available to the academic community, such as virtual campuses, remote work tools, the corporate authentication system and institutional e-mail accounts, be used. Biometric data cannot be used to identify students.

2) It is good practice to ask students at the beginning and/or throughout the session to disable their camera and microphone except when they intervene.

3) Ideally, in remote classes students should intervene at the end of the teacher's explanation or via chat during the session. In this way, if the session is recorded, the section in which students did not intervene can be made public. Because this is impractical, if it is necessary to record the session, including students' interventions, the recording must be stored on the teaching intranet and access restricted to students enrolled in the subject. The recording must be deleted once the academic year ends. For other cases and/or uses, students must be informed and their consent obtained.

4) If obtaining images of students is planned or necessary for the session, students must be told to make sure that any personal objects that they wish to keep private are kept out of view. We recommend that professors do the same.

5) Students must be informed at the beginning and/or during the session that recording and/or broadcasting the session on the internet (YouTube, social networks, etc.) in part

or in whole is prohibited. This also applies to any other medium, except for the teaching purposes foreseen in the framework of the subject. A warning such as the following may be included: © Universitat Politècnica de Catalunya, 2020. All rights reserved. It is strictly forbidden to record, broadcast, communicate or publish this session on the internet or by any other equivalent means.

6) When the class must be recorded, those present must be informed of the recording beforehand, and the fact that they have been warned must be recorded. This information must include the purpose of the recording. A good way to do this might be to read or display the following information at the start of the session:

• *Due to the temporary suspension of on-campus teaching activity at the UPC, we inform you of the conditions of use of this video recording:*

a) The session will be recorded so as to later provide students with the content.

b) We guarantee that, other than in subsequent cases in which this is expressly authorised, recordings will only be used in the classroom assigned to the course and during the period assigned to the course.

c) We recommend that those present disable the camera on their device if they do not want other participants to see them.

d) Recording the session, as well as reproducing or disseminating it (for example, on social networks or services for sharing class notes), in whole or in part, regardless of the means or device used, is prohibited. Any misconduct is a violation of current regulations and may lead to legal liability.

B. Specific recommendations for distance assessment

1) For students to make adequate progress in their educational activity, as well as to effectively distribute their workload, continuous assessment is recommended using the tools and resources available at our university, the course guides and tools specifically developed for this semester. The periodic assessment of asynchronous activities by means of multiple-choice tests, exercises and individual and teamwork is expected, in order to reduce, as far as possible, the weight of the final exam in the final mark for the subject. In general terms, the weight of the final exam must not exceed that established in the UPC's general and specific regulations approved by the competent governing bodies.

2) The University has virtual teaching platforms such as ATENEA and the FIB's Racó, which, together with the G Suite for education that was recently activated for the entire UPC community, will allow teaching activity to be maintained for as long as the lockdown lasts. These platforms allow professors and students to provide their identity details when they access them with their UPC credentials.

3) Changes to the organisation, content and assessment of each subject will be detailed in addenda to the course guides. Students will be informed sufficiently in advance, preferably through ATENEA, the *racons* or other means commonly used in the subject.

4) Continuous assessment should be prioritised using means of assessment (assignments, tests, etc.) that protect students' privacy as much as possible. In the event that subject coordinators consider it necessary to programme synchronous assessment tests that require students' identity to be checked and for them to

monitored remotely (for example, final exams), the restrictions and limits established in personal data protection laws (the GDPR and the LOPDGDD) must be taken into account, which translates into the following considerations:

a. Monitoring (not recording) students by video conference continuously or sporadically while they are taking an exam is considered legitimate and may be done.

b. Recording students' image on an ongoing basis while they are taking an exam is not legitimate and must not be done, as it is not a proportionate measure. However, it is considered legitimate to record a close-up of the students at the beginning and/or end of the exam, and of the exam papers, and this may be done to lend robustness to the process of identification and authentication. It is also considered legitimate to record students with an identification document such as the UPC card. If identity cards, such as the DNI or NIE, or passports are recorded, it is advisable to ask students to display just their name and photo and for any other personal data to be hidden. We recommend removing any personal objects that are considered personal or private from the background of the image.

c. Professors are allowed to implement measures that strengthen the control and authentication in exams that are conducted remotely. Requesting the resources needed to scan handwritten documents is considered legitimate and may be done. There are options for installing scanning systems such as Drive on your mobile with a UPC ID. Other options must take into account the limitations specified in the *ICT Security and Personal Data Protection Criteria in Class and/or Remote Assessment.*

The ATENEA platform and the G Suite applications allow exam papers to be published and exams to be delivered in compliance with the requirements of the GDPR and the LOPDGDD. It is also legitimate for professors to select exams randomly for students to defend their answers by video conference. However, in the current circumstances it is unadvisable to request that students install additional software, such as navigation blocking systems or others, on their computers (which can be shared with other users in the private environment), because this is not sufficiently legitimate and cannot be to demanded in all cases. Some students could legitimately refuse, and additional procedures would need to be established for them.

d. The UPC's ICT services will provide a list of programs that comply with the GDPR and LOPDGDD and the security requirements for handling exams. For applications that are not included, a report will be required beforehand. Contact ATIC (by submitting a ticket or calling 93 401 62 13) with any questions you might have.

e. Students must be informed of the procedure and requirements to participate in exams in accordance with the instructions in the document *ICT Security and Personal Data Protection Criteria in Class and/or Remote Assessment.* The legitimate interest of this personal data processing is the fulfilment of a mission carried out in the public interest (Organic Law 6/2001, of 21 December, on Universities), which implies that the interested party's consent is not required.

f. Students' actions must aid the work of teaching staff and be guided by the principles of cooperation, responsibility, honesty, integrity and others, in accordance with the University Student Statute and the Code of Ethics and Good Practice for Staff and Students of the Universitat Politècnica de Catalunya.

Therefore, the guidelines contained in this document should always be interpreted in light of the duty to collaborate in facilitating the University's educational and assessment activities of everyone involved.

g. The methodology, conditions and procedure of the remote exams must be communicated in advance so that students can verify that they meet the technical requirements. The ICE will provide an exam paper and samples to validate the process in ATENEA, the *racons* and standard G Suite applications. An alternative assessment system and communication system should be provided for incidents (the absence of ICT resources and computer compatibility or connectivity problems, for example) before or during exams. It is good practice for students to log in on their mobiles and computers simultaneously, as this helps to solve issues quickly during the exam.

h. If it is considered appropriate to give students a contact telephone number, so as not to give their personal telephone numbers the UPC's teaching and research staff may, exceptionally and during the state of alarm, request that calls to their office be redirected to their personal mobile phones by contacting ATIC (by submitting a ticket or calling 93 401 62 13), without the need for authorisation from the head of the unit, who will receive a message to this effect. This measure will be reversed when the situation returns to normal and the standard procedure and conditions are reinstated.

i. It is considered good practice to allow exams to be submitted after the end of the exam; possible penalties should be evaluated and communicated based on the justification for the delay, if applicable. This allows incidents to be dealt with more efficiently.

j. Biometric data may not be processed, because it is not considered legitimate for the UPC to process this special class of data. In the same sense, it is not considered sufficiently legitimate to view or record a widescreen view of the personal space occupied by students.

k. In all cases of synchronous assessment tests that require students' identity to be checked and for students to be monitored remotely, in accordance with the document *ICT Security and Personal Data Protection Criteria in Class and/or Remote Assessment* the interested parties must be informed at two specific moments:

a. When they are sent an e-mail with the link to the session.

b. When they log in.

To this effect, the statement "All the information on compliance with personal data protection regulations that pertain to this test may be consulted in <LINK>" must be included at the end of e-mails containing information and providing the link to sessions. The link must lead to a document that contains information on the subject (ATENEA, the Racó or similar), with the basic data protection information table. Preferably, a single table for each subject that includes all the remote events planned will be provided. The information that must be provided includes:

Identity and contact details of the controller	Universitat Politècnica de Catalunya The name of the school or unit and a link to the web page with contact details The e-mail address of the subject coordinator (or a list of the e-mail addresses of the professors assigned to each specific group or test)
Contact details of the	Universitat Politècnica de Catalunya.

data protection officer	(https://www.upc.edu/normatives/ca/proteccio-de-dades/normativa-europea-de-proteccio-de-dades/dades-de-contacte-del-delegat-de-proteccio-de-dades)
Purposes of the processing	[F03.21 Virtual campus management](https://rat.upc.edu/ca/registre-de-tractaments-de-dades-personals/F03.21) (https://rat.upc.edu/ca/registre-de-tractaments-de-dades-personals/F03.21) **Class / remote assessment session (or class / remote assessment session for the subject XXX) at the school XXX, 2020**
Legitimate interests	Based on the fulfilment of a mission carried out in the public interest (Organic Law 6/2001, of 21 December, on Universities)
Recipients or categories of recipients	Your first and last name or session ID will be visible to other participants when you attend the session. Your image and/or voice will be accessible to other participants if you activate the camera and/or microphone during the session. Your data will not be transferred to third parties unless it is legally binding to do so.
Rights	[Right of access by the data subject, right to rectification or erasure, right to restriction of processing, right to object, right to data portability.](#) (https://www.upc.edu/normatives/ca/proteccio-de-dades/normativa-europea-de-proteccio-de-dades/drets)
Period for which the personal data will be stored	As needed for any of the purposes that are described in our retention policy. (https://www.upc.edu/normatives/ca/proteccio-de-dades/normativa-europea-de-proteccio-de-dades/politica-de-conservacio-de-les-dades-de-caracter-personal)
Complaint	If you have been unable to exercise your rights to your satisfaction, you can file a complaint with the APDCAT: apdcat.gencat.cat

5) The technical and organisational measures implemented must aim to guarantee the integrity, confidentiality and traceability of students' answers to exams.

C. ICT recommendations

In order to adapt the monitoring and assessment of teaching to an online environment, within the framework of the situations and recommendations established by the UPC's Executive Council and data protection officer, the ICT services recommend using the official corporate tools that are available to the community, which are, in the specific case of teaching, the ATENEA virtual campus and the G Suite platform for education.

1. ATENEA: the UPC's virtual campus allows for a wide variety of online activities both in real time and in deferred form, and it safeguards the principles of confidentiality, integrity, authenticity and traceability. Therefore:

● It is the recommended place for hosting resources and carrying out online activities (questionnaires, tasks, forums, etc.), because students are obliged to provide their credentials (username and password), visibility is limited to the members of a classroom and records are kept of all the activity.

● It has a plagiarism detection tool (Urkund).

● It restricts access to activities and resources according to certain criteria: a date, a mark, membership of a group or the completion of an activity.

2. G Suite for Education: the G Suite collaborative application suite is offered with corporate accounts (rather than personal Gmail accounts) under an agreement with the UPC. Therefore:

● They must be used from the @upc.edu and @estudiantat.upc.edu accounts created in G Suite.
The recommended applications (Meet and Drive) have been integrated with automatically created official enrolment groups on the ATENEA platform, which makes it easier for members to limit their access and/or visibility.

● Documents and files containing personal data must not be shared with users outside UPC domains without the consent of those affected.

3. Google Meet: this is the recommended video conferencing solution integrated into the G Suite platform. It has a chat function. Recommendations:

● Invitations to video conferences can be sent by different means. We recommend sending the link to students via ATENEA. (This way there is evidence of the invitation.)

● Until 1 July 2020, video conferences can be saved in the organiser's "Meet Recordings" folder.

● Its use may involve users being identified and their voice and/or image being recorded. Therefore, for all recorded video conferences the recommendations on computer security and data protection must be followed, and participants must be informed that the session is being recorded and the purpose of the recording.

● <u>If students do not speak, their data are not recorded</u>.

● To share a recorded video conference with students, we recommend publishing the link in ATENEA.

4. Google Drive: the solution for collaborative storage and file sharing and editing. It offers unlimited space. Recommendations:

● To facilitate the sharing of documents and files, during the COVID-19 emergency sharing with users external to UPC domains (@upc.edu and @studentat.upc.edu) is enabled. However, it must be kept in mind that content that includes personal data must not be shared outside the UPC community.

5. Video storage and publication

● We recommend storing videos in official repositories outside ATENEA (Drive, the LISA YouTube channel) and linking to them from the virtual campus classrooms.

● We recommend posting the video as HID. (Only people with the link to the video will be able to see the video.)

● If the video is stored in Drive we recommend the option that disables its possible download.

● All these recommendations are binding if the videos contain students' personal data and students have not consented to their public dissemination.

6. Scanning and remote session recording tools

● To scan documents such as written exams if you do not have a scanner, use the Google Drive application on your mobile with your UPC credentials, so that the PDF generated is stored in the UPC repository on Google. It is very easy to use: just open the application, press the "+" icon and follow the instructions.

● To record remote sessions, we recommend using Google Meet, taking into account all the considerations discussed above.

7. Other general ICT considerations

a. Students' identity in the recommended corporate ICT tools is accredited with UPC credentials (username and password).

b. The UPC does not currently have any student identification system that uses facial recognition (such as Respondus, Smowl, Proctor Exam, etc.). These systems process biometric data that are part of a special class of personal data with a level of protection that is not currently implemented at the UPC.

c. Any other tool or system (browser blocking, desktop sharing, etc.) that lies outside these recommendations will require analysing risks to data protection and information security.

d. The tools recommended by the UPC comply with data protection regulations. Users use them under their own responsibility.

e. Using a virtual teaching environment implies that identification data, images, audio and comments in a forum of teaching staff and students may be processed. The tools themselves do not guarantee that the data are protected, and you must keep in mind the purpose for which they are used. For this reason it is vitally important to consult the recommendations on computer security and data protection.

D. Frequently asked questions and additional considerations
This section addresses the considerations and recommendations set out in the previous sections, which are reformulated in view of the questions that have we have been asked most frequently.

Can students be asked to show the setting where they will take exams to make sure that there is no one helping them and that the devices that they might

consult (e.g. cell phones) are not available to them?

The fundamental rights of individuals to privacy must be respected. These rights may differ when the setting is a classroom or a personal, private and intimate space.
In any case, these rights are not unlimited, and a commitment must be established. The visualisation (without recording) of students' assessment for control purposes may be considered proportional in the exceptional situation in which we find ourselves; therefore, if we apply the same criteria as we do in face-to-face assessment, we could conclude that it is legitimate and that it may be done.

However, the continuous recording of an exam may be disproportionate, as this type of personal data processing does not occur in an on-site exam. It is therefore necessary to determine the criteria that must be weighed up in relation to conducting and monitoring an exam and students' right to their honour, their own and their family's privacy and their image. Without these criteria, there can be no weighing up of fundamental rights, and therefore it is not legitimate to record the entire exam and this should not be done.

Rather, it may be considered legitimate, exclusively for the purpose of tracing students' delivery of the answers to an exam, to record students and their answers to the exam once the exam is over, and this may be done.

It may also be considered legitimate to record a close-up of students to identify them at the beginning of an exam, in order to lend robustness to the process of identification and authentication.

Can students be asked to show their ID to the camera to check their identity?

The proportionality of this measure must be evaluated, given that the rest of the participants in the session will also be able to see the student's ID.

If the coordinator or professor deems it necessary to reinforce the procedure for identifying students, it is legitimate to record the student with an identification document such as the UPC card. If you use your DNI, NIE or passport, it is advisable to ask students to display just their name and photo and for any other personal data to be hidden.

If professors realise that a student is looking up information or receiving help that has not been authorised, how should they proceed?

It will be necessary to apply the same criteria as in face-to-face assessment, as established in the academic regulations.

3.1.2 Academic Regulations for Bachelor's and Master's Degrees: irregular actions potentially leading to a significant variation of the marks obtained by one or more students will be considered a breach of the assessment regulations. Such behaviour will result in a descriptive mark of "Fail" and a numerical mark of 0 for the examination in question and the subject, without prejudice to any disciplinary proceedings that may result from that behaviour.

How should one proceed if a student does not have the necessary computer resources to attend a class and/or exam?
Technical and organisational measures to facilitate student participation must be established before the session. Section 3.1.2 of the Academic Regulations for Bachelor's and Master's Degrees must be considered: students have the right to be

assessed in all of the subjects for which they are enrolled and to the curricular adaptations that ensure their real and effective inclusion.

It should be understood that students who have not cancelled or modified their enrolment by the corresponding deadline continue to be committed and are able to follow teaching and assessment, despite the restrictions stemming from the current situation. In the event that, before an exam, a student claims to be unable to take it due to unforeseen circumstances the school must establish an appropriate procedure: to change the date of the exam or the exam type.

How should one proceed if during an exam and/or class a student needs to temporarily be absent?

The same criteria as for a face-to-face exam, as established in the academic regulations, must be applied by the school and/or professor. This usually involves a communication from the professor in which permission is or is not granted.

How should one proceed if during an exam the network connection fails or the tool used malfunctions?

The technical and organisational measures necessary for this type of situation must be established before the session.

Professors must establish a secure communication mechanism before the start of the exam, so that students who have any problems can inform them during the exam. Professors must establish an appropriate procedure and change the date of the exam or the exam type.

Can unique biometric identification systems be used to identify students?

Unique biometric identification data are personal data that the University does not collect from students. These data are part of the special class of data established in the General Data Protection Regulation (EU 2016/679), and risk assessment may be required for them to be processed. Therefore, unique biometric identification systems for students cannot be used at this time.

Can students be asked to install a tool on their computers that blocks certain features (such as browsing through links other than those authorised, copying and pasting, sharing their desktop, etc.)?

Yes, but the risks of the blocking tool must be analysed to establish whether it is processing personal data on the student's computer (for example, the IP address, configuration data, browsing history, etc.), which data are being processed and their class, whether there are recipients and how long they will be stored for. However, in the current circumstances it is not advisable, as it is not sufficiently legitimate or enforceable in all cases.