UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Seguretat TIC i Protecció de Dades

ICT security and personal data protection criteria in class and/or remote assessment

1. Object

This document establishes the criteria for ICT security and personal data protection for classes and/or assessment using remote working tools, in order to guarantee the right to personal data protection in these actions and exceptional circumstances as a result of the state of alarm.

2. Scope and legal framework

These criteria affect virtual classes and / or virtual assessment conducted by means of computer and telecommunications tools at the UPC in the framework of the state of alarm decreed on 14 March 2020.

These criteria are an accompaniment to the decision on the urgent and extraordinary measures to guarantee teaching at the UPC during the health emergency taken by the Governing Council on 1 April 2020 (Decision CG/2020/02/05).

Organic Law 4/1981, of 1 June, on states of alarm, exception and siege, allows measures to be taken with the limitations indicated in Article 11, without these measures involving in any case the suspension of rights and freedoms.

Data protection is a fundamental right and is classified as an essential autonomous right that is independent of the right to personal and family privacy by the Constitutional Court (STC 292/2000, of 30 November). This right must be guaranteed even in the current state of alarm caused by COVID-19. Accordingly, Royal Decree 463/2020, of 14 March, which declares the state of alarm, does not suspend the right to data protection, nor do any rules issued subsequently. In order to safeguard this fundamental right, during the state of alarm and extensions thereof, Organic Law 3/2018, of 5 December, and the General Data Protection Regulation are fully applicable, in addition to Organic Law 1/1982, on the Civil Protection of the Right to Honour, to personal and family privacy and to one's own image.

This was stated by the legal office of the Spanish Data Protection Agency in Report 0017/2020: *"the processing of personal data in these health emergency situations, as mentioned at the beginning of this report, continues to be regulated in accordance with the legal instruments for the protection of personal data (RGPD and Organic Law 3/2018, of 5 of December, for the Protection of Personal Data and guarantee of Digital Rights, LOPDGDD), so all data protection principles, contained in article 5 GDPR, are applied, including the principles of legality, loyalty and transparency, purpose limitation (in this case, the safeguarding vital/essential interests of natural persons), accuracy, and of course, and we must especially emphasize it, the principle of data minimization. Regarding this last aspect, it is necessary to make express reference to the fact that the data processed must be exclusively limited to those necessary for the intended purpose, without such processing being extended to any other personal data not strictly*

necessary for said purpose, without being able to confusing convenience with necessity, because the fundamental right to data protection continues to apply normally."

Accordingly, and in order to respect the rights of all members of the university community, the University, in exercising its right to autonomy, has reorganised its activities and is using the tools and systems available to it to continue with its teaching activity. All members of the community are required to actively collaborate in the actions taken. As regards remote classes and assessment, student cooperation is essential, as it is essential that the University provide them with the necessary means to participate if they do not have the technical means to do so.

With regard to the involvement of the rights and duties of university students that are likely to be transferred to the current context, we must mention Royal Decree 1791/2010, of 30 December, which approved the University Student Statute. Article 13 regulates students' obligations, including their obligation to cooperate in the University's activities, their responsible participation and their contribution to improving the functioning of the University. The Code of Ethics and Good Practice for Staff and Students of the Universitat Politècnica de Catalunya (approved by Governing Council Decision no. 106/2011) expressly foresees that the principles that govern the University's activity with regard to its staff and students are those of cooperation, joint responsibility, honesty and integrity, among many others. Article 3.4 of the Code, which concerns students, states the following:

"Students must show a participatory approach in all educational activities, facilitate the work of professors, and evaluate the professors' activities when asked. They must also recognise the value of personal effort in examinations and assessments and promote this attitude among fellow students. Furthermore, they should seek to participate in the representative and governing bodies of the University that correspond to them."

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.

3. Guarantees of ICT security and personal data protection

The measures adopted by the schools as a result of the implementation of the guidelines issued by the management, and under the general criteria established by the Office of the Vice-Rector for Academic Policy, must comply as far as possible with the technical and organisational measures that guarantee information security and the protection and traceability of personal data.

The guarantees of ICT security are those indicated for the public administrations in Royal Decrees 3/2010 and 951/2015, which regulate the National Security Scheme.

CONFIDENTIALITY: The consequences of disclosure to unauthorised persons or who do not need to know the information should be considered.

INTEGRITY: The consequences of modifying the information for someone who is not authorised to update the information must be considered.

AUTHENTICITY: The consequences the information not being authentic must be considered.

TRACEABILITY: The consequences of not being able to check who has accessed or modified the information later must be considered.

The guarantees of personal data protection are those indicated in the General Data Protection Regulation (EU) 2016/679:

The principles of data protection apply to all information regarding an identified or identifiable natural person.

LEGITIMACY, LOYALTY AND TRANSPARENCY: Personal data must be processed in a lawful manner. The principles of fair and transparent processing require that the interested party be informed of the processing and its purpose. If personal data are obtained from the interested parties, they must also be informed if they are obliged to provide it and the consequences of not doing so.

LIMITATION OF THE PURPOSE: Personal data must be collected for specific, explicit and legitimate purposes, and they must not subsequently be processed in a way that is incompatible with these purposes.

DATA MINIMISATION: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

ACCURACY: Personal data must be accurate and, if necessary, updated; reasonable measures must be taken to delete or rectify without any delay the personal data that are inaccurate for the purpose for which they are treated.

LIMITATION OF THE RETENTION PERIOD: The personal data must be kept in a way that allows them to identify the interested parties for a period not longer than necessary for the purposes of the processing of personal data.

INTEGRITY AND CONFIDENTIALITY: Personal data must be treated in a way that guarantees adequate security, including protection against unauthorised or unlawful treatment and against loss, destruction or accidental damage, through the application of appropriate technical or organisational measures.

4. Information and personal data in a class using remote work tools

The minimum information that may be processed in a class using remote work tools, and which is the subject of this report regarding ICT security and personal data protection criteria, is the following:

- Announcement of the session
- Registration of the access of each student to the class (recommended)
- Voice and image of the professor
- Work environment of the professor
- Professor ID in the computer tool
- Teaching content of the topic to be explained
- Voice and image of the students

- Work environment of the students
- Student ID in the computer tool
- Questions or comments from students
- Recording, if appropriate, of the session (without student intervention)
- Recording, if appropriate, of the entire session (with student intervention)

5. Information and personal data in assessment using remote work tools

The minimum information that may be processed in assessment using remote work tools, and which is the subject of this report regarding ICT security and personal data protection criteria, is the following:

- Announcement of the assessment
- Registration of the access of each student to the class
- Work environment of the professor
- Professor ID in the computer tool
- Exam questions for the subject to be assessed
- Voice and image of the students
- Work environment of the students
- Student ID in the computer tool
- Questions or comments from students
- Answers of the students to the exam
- Recording, if appropriate, of the exam (with student intervention)
- System for submitting the answers to the exam

6. Risk analysis

The tools currently available to the UPC community have already been evaluated from the point of view of risks to ICT security and data protection.

In the case of using tools other than those made available by the UPC, a risk analysis must be performed prior to its use, in order to guarantee ICT security and personal data protection, as detailed below. This should be done by those who have decided to use the particular tool, if possible with the involvement of the school.

This risk analysis must allow us to evaluate the guarantees established in Section 3 of this document and establish the technical and organisational measures necessary to mitigate the risks.

Risks associated with CONFIDENTIALITY:

It is necessary to evaluate whether the tool used allows the data described in sections 4 and 5 of this document to not be disclosed to unauthorised third parties or who do not need to know the information.

From all the information and personal data, it will be necessary to guarantee that the tool used maximises access to the session so that only the people who are present can access it.

In addition, if the class is recorded with student intervention, this recording must only be accessible to participants, and the necessary technical measures must be taken to prevent the video from being downloaded.

With regard to students' answers to exams, the tool and / or technical and organisational measures used must guarantee confidentiality as they would for on-site exams.

Risks associated with INTEGRITY:

Of the information and personal data of the classes and the exams, it is necessary to consider, in particular, the completeness of the announcements of remote sessions, of the recording of the sessions and of students' answers to exams, as well as the consequences that their modification by someone who is not authorised to update the information might have. Risks of accidental loss, destruction or damage must also be evaluated through the application of appropriate technical or organisational measures.

Risks associated with AUTHENTICITY:

In terms of authenticity, the authenticity of participants' identities must be analysed, as well as whether students' answers to exams have been written by their author. The consequences of the information not being authentic must be considered.

To minimise the risks associated with authentication, the credentials used to access the UPC's information systems (UPC username and password, institutional e-mail, G Suite identifier) must be used.

Risks associated with TRACEABILITY:

The tool used for classes and/or assessment must keep a record of when they took place, who participated and the computer from which they were made available to participants. With regard to recordings, it will be necessary to know who has accessed and/or modified them, in order to establish the consequences that a failure to track the subsequent use of this information and personal data might have.

Risks associated with LEGITIMACY, LOYALTY AND TRANSPARENCY:

The processing of the personal data described above for classes and assessment is that which is defined in the UPC's Register of Processing Activities as F03.21 Virtual campus management.

The personal data described in sections 4 and 5 of this document are already included in the Register of Processing Activities; therefore, the risk associated with legitimacy, loyalty and transparency is that the tool used in the classes or assessment, as well as the technical and organisational measures used, include other types of personal data or that the interested party is not informed of the processing and its purposes. There is also the risk that they will not be informed that they are obliged to provide them and of the consequences of not doing so.

Risks associated with the LIMITATION OF THE PURPOSE:

The main risk associated with limiting the purpose is that the tool used for classes or assessment and the technical and organisational measures followed allow processing that is incompatible with the purpose established in the processing to support teaching and learning:

● Communication between students and teaching staff and between students themselves.

● Completion of activities and access to the resources proposed by teaching staff.

● Assessment by teaching staff.

As an example, if the recording of a class with student interventions is NOT restricted to the students on the course this would constitute a violation of the principle of limitation of purpose.

Risks associated with DATA MINIMISATION:

The main risk associated with the minimisation of personal data is that the tool used for classes or assessment and the technical and organisational measures followed process more personal data than is needed.

It will be necessary to determine whether students' image and voice must be featured in the class. We must ask why participation must feature visuals and sound. We must ask whether we can achieve the same teaching result by logging just the image and voice of the professor and the presentation, and whether students can participate with their camera and microphone turned off and using the chat function.

Risks associated with ACCURACY:

The main risk associated with the accuracy of personal data is that the tool used for classes or assessment and the technical and organisational measures followed allow personal data that do not belong to the students who are enrolled in a particular subject to be processed.

Risks associated with the LIMITATION OF THE RETENTION PERIOD:

The risk associated with limiting the retention period is that recordings of classes and/or assessment are stored beyond the time required for the purposes of processing personal data.

7. Legitimacy of personal data processing

Whenever the criteria set out in this document are followed, the legitimate interest of the 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.

● Communication between students and teaching staff and between students themselves.

● Completion of activities and access to the resources proposed by teaching staff.

● Assessment by teaching staff.

It should be borne in mind that, if it is foreseen that the personal data will be used for a purpose other than that for which it was gathered, before subsequent processing the interested parties must be provided with information on this other purpose and any additional pertinent information so that they can exercise their rights, including, if necessary, the right not to give their consent for this new purpose.

8. Information to be provided to students

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.

The basic data protection information to be provided is as follows:

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 data protection officer	Universitat Politècnica de Catalunya. (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) **Remote class / assessment (or remote class / assessment 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

The information marked in yellow in the table above must be adapted by each school.