RULES AND REGULATIONS OF THE INSTITUT CATHOLIQUE DE TOULOUSE APPLICABLE TO STUDENTS AND AUTHORISED EXTERNAL VISITORS

Adopted by the ICT School Council on 15 May 2024

PREAMBLE

The Institut Catholique de Toulouse (ICT) is an Etablissement d'Enseignement Supérieur Privé d'Intérêt Général (EESPIG) with its head office at 31, rue de la Fonderie BP 7012 31068 Toulouse Cedex 7. It is an association under the French Law of 1901, recognised as being of public interest by the decree of 22/11/2001 and registered with the Préfecture de la Haute Garonne under N° RNA W313006581 - SIRET n° 776 944 100 00010 - Code APE : 8542Z.
The Institut Catholique de Toulouse is also a continuing education organisation registered with the Préfecture under the number 73 31 00401 31.

The ICT offers and provides short and long courses in initial training or lifelong continuing education, with or without sandwich courses. These courses can take place on one of the ICT's 2 campuses:

- The Toulouse campus, spread over 3 sites :
  - 31, rue de la Fonderie 31000 TOULOUSE ;
  - 7-8, Place du Parlement 31000 TOULOUSE ;
  - 22, rue des Fleurs 31000 TOULOUSE.

- Bordeaux campus: 2-8 Allée Marianne Loir 33 800 BORDEAUX.

SUBJECT AND SCOPE OF APPLICATION OF THE RULES

The purpose of these internal regulations is to define the general and permanent rules governing health, safety and discipline on the Toulouse campus.

It applies to all learners enrolled at the ICT, whether they are :

- Learners in initial training ;
- Learners under apprenticeship contract or apprenticeship contract ;
- Continuing education trainees ;
- Free listeners.

As well as authorised external visitors.

It also defines how learners are represented.

For continuing education trainees, in accordance with article R 6352-1 of the French Labour Code, when the training takes place in a company or establishment that already has internal regulations, the health and safety rules applicable to trainees are those set out in these regulations.
The ICT's internal rules can be consulted on Scolaweb (https://scolaweb.ict-toulouse.fr) and posted at the reception desks on the three sites.

SECTIONS APPLICABLE TO ALL LEARNERS AND AUTHORISED VISITORS

SECTION 1: GENERAL PRINCIPLES

1.1. HYGIENE AND SAFETY

Preventing the risk of accidents and illness is imperative and requires everyone to comply with all applicable regulations.

health and safety regulations in force within the establishment.
The ICT Rector is responsible for security on the school premises.
All students registered with the ICT or authorised visitors must ensure their personal safety and that of others by scrupulously respecting the general and specific safety and hygiene instructions in force at the training centre. In the event of proven non-compliance, disciplinary action may be taken.

1.1.1. SAFETY INSTRUCTIONS

Any learner enrolled at the ICT or any authorised visitor present on ICT premises must imperatively take read and comply with the fire safety instructions for the building they a r e in. They are posted in the building and presented in the "Safety instructions" document (in appendix 1) so that everyone is aware of them. They include a map s h o w i n g t h e location of fire extinguishers and emergency exits.
Like all members of the university community, all students enrolled at the ICT and all authorised visitors are required to comply immediately with the order to evacuate the premises and to respect the instructions given by the Head of School or his/her representative. If the fire alarm goes off, everyone must immediately evacuate the premises and wait for instructions before re-entering.

In order to ensure free access to the buildings' emergency exits, it is forbidden to park or position furniture or equipment in the circulation areas used to evacuate the occupants of the lCT premises. It is forbidden to park vehicles in the courtyard at 31 rue de la Fonderie without authorisation.
Corridors and staircases must be kept free of any objects or furniture that might impede passage.

It is strictly forbidden to render an exit or emergency exit unusable. Fire safety installations and equipment (fire extinguishers, alarm systems, etc.) are designed to protect people's lives in the event of a disaster.

Failure to comply with these instructions, or wilful damage to this equipment, exposes the offender to disciplinary and possibly criminal sanctions for endangering the lives of others (article 121-3 of the French Criminal Code). Any unjustified triggering is also punishable under criminal law (article 322-14 of the French Criminal Code).

The organisation periodically of evacuation drills on lCT premises is a regulatory obligation which no member of the university community can avoid, on pain of incurring disciplinary sanctions.
It is everyone's responsibility to ensure that their behaviour and activities prevent the risk of fire (storage of paper, use of flammable products, electrical appliances, etc.) and to report any abnormalities to the ICT main reception desk (31, rue de la Fonderie, 05 61 36 81 00). Fans must be unplugged after use.

1.1.2. INSTRUCTIONS IN THE EVENT OF AN ACCIDENT, MEDICAL EMERGENCY OR HEALTH CRISIS

Any accident or incident must be reported immediately by the victim or any person witnessing the accident to the ICT main reception at 31, rue de la Fonderie (05 61 36 81 00).

In the event of a health crisis announced by the government, any learner enrolled at the ICT or any authorised visitor present on the ICT premises must comply with the instructions posted within the ICT in accordance with ministerial directives.
These rules apply in all areas of the ICT (classrooms, corridors, premises, etc.).

student life, self-service restaurant, shared workspaces, ICT café, library.

1.1.3. TOBACCO, ALCOHOL, DRUGS, DANGEROUS OBJECTS NO SMOKING

In accordance with decree no. 2006-1386 of 15 November 2006 (article R. 3511-1 of the public health code), issued in application of law no. 31-32 of 10 January 1991, all premises in the ICT buildings are entirely non-smoking. Smoking is strictly prohibited on the ICT premises, including courtyards, gardens and access porches.

The use of electronic cigarettes i s also prohibited on ICT premises. However, in order to limit the risks associated with the presence of people on the public highway, the ICT has set up two outdoor smoking areas (located on the Fonderie site) which must be respected.
Users are required to put their cigarette butts in the ashtrays provided.
Failure to comply with these provisions may result in disciplinary action.

SALE AND CONSUMPTION OF ALCOHOL, ORGANISATION OF FESTIVE EVENTS

It is forbidden for students to enter or remain on the premises in a state of intoxication, or to bring in alcoholic beverages.
The entry or presence on the premises of a person who is clearly intoxicated must be reported immediately to the site reception, who will refer the matter to the person in charge.
The consumption and sale of alcohol is prohibited on the ICT premises.
Failure to comply with these provisions may result in disciplinary action.
Exceptional dispensation may be granted by the ICT Rector. Any organiser of a festive event for ICT students within the ICT must first submit a request for authorisation to the Rector.

INTRODUCTION OF HAZARDOUS SUBSTANCES

It is forbidden to bring onto the ICT sites any substance (in particular narcotics), any material or instrument that is dangerous (in particular weapons), illegal, harmful to health or contrary to public health or public order requirements, unless expressly authorised by the competent authorities.

Such acts will give rise to disciplinary proceedings that are independent of any criminal proceedings that may be brought.

1.1.4. BEHAVIOUR AND RESPECT FOR PEOPLE

DRESS AND BEHAVIOUR

When attending classes or examinations, and when using common areas (cafeteria, shared work areas, ICT café, library, foyer, etc.), students must dress decently and behave with respect for people and property.

In particular, learners must comply with Law no. 2010-1192 of 11 October 2010 prohibiting the concealment of the face in the public space.

During examinations, the wearing of clothing must not make it impossible or difficult for learners to be identified, or be likely to give rise to doubts about such identification, and must not conflict with the requirements of the organisation and smooth running of the tests.

The basic rules of civic-mindedness, politeness, respect, hygiene and safety towards everyone, inside and around the ICT, are everyone's responsibility for the well-being of all:

- A reasonable noise level must be maintained in front of the ICT for the sake of good neighbourliness. The same applies inside the ICT, out of respect for the various members of the university community;

- For reasons of personal safety (traffic accidents, Vigipirate plan, etc.) and civic-mindedness (particularly towards neighbours and people using the public space), please do not remain in groups in front of the ICT entrance, do not obstruct the passage of people and vehicles, do not leave litter on the public highway (particularly cups, cigarette butts, etc.) and use the dedicated equipment installed inside the ICT or on the public highway;

- Learners must respect course start and end times.
The ICT reserves the right to modify course timetables according to service requirements. Students must comply with these changes.
In the event of absence or lateness, students should notify the school as soon as possible by contacting the secretariat of their faculty, school or institute;

- The use of mobile phones during lessons and any other university activity is strictly forbidden (unless authorised by the teacher in a specific context or in cases of force majeure);

- Unless expressly exempted, it is strictly forbidden to record or film training sessions.

DISCRIMINATION

Under article 225-1 of the French Criminal Code,
"Discrimination is any distinction made between individuals on the basis of their origin, sex, family status, pregnancy, physical appearance, particular vulnerability resulting from their economic situation, whether apparent or known to the perpetrator, surname, place of residence, state of health, loss of autonomy, disability, genetic characteristics, morals, sexual orientation, gender identity, age or political opinions, their trade union activities, their status as a whistleblower, facilitator or person in contact with a whistleblower within the meaning, respectively, of I of Article 6 and 1° and 2° of Article 6-1 of Law 2016-1691 of 9 December 2016 on transparency, the fight against corruption and the modernisation of economic life, their ability to express themselves in a language other than French, their actual or assumed membership or non-membership of a particular ethnic group, nation, alleged race or religion.

Any distinction made between legal persons on the basis of origin, sex, family status, pregnancy, physical appearance, particular vulnerability resulting from the economic situation, apparent or known to the perpetrator, surname, place of residence, etc. also constitutes discrimination, state of health, loss of autonomy, disability, genetic characteristics, morals, sexual orientation, gender identity, age, political opinions, trade union activities, status as whistleblower, facilitator or person associated with a whistleblower, within the meaning of I. de l'article 6 et des 1° et 2° de l'article 6-1 de la loi n° 2016-1691 du 9 décembre 2016 précitée, de la capacité à s'exprimer dans une langue autre que le français, de l'appartenance ou de la non-appartenance, vraie ou supposée, à une ethnie, une Nation, une prétendue race ou une religion déterminée des membres ou de certains membres de ces personnes morales."

Such acts will give rise to disciplinary proceedings that are independent of any criminal proceedings that may be brought.

HAZING AND MORAL HARASSMENT, SEXIST AND SEXUAL VIOLENCE

Hazing offends the dignity of others. In accordance with article 225-16-1 of the French Criminal Code, it constitutes an offence and is defined as follows: "*Except in the case of violence, threats or*

of sexual offences, the fact of a person causing another person, against their will or not, to undergo or commit humiliating or degrading acts or to consume alcohol excessively, during events or meetings linked to the school and socio-educational environment, is punishable by six months' imprisonment and a fine of 7,500 euros".
Penalties are increased if the victim is particularly vulnerable.

Hazing is also a disciplinary offence that may result in a penalty.

Any form of moral harassment within the meaning of Article 222-33-2 of the French Penal Code ("the act of harassing another person by repeated comments or behaviour with the purpose or effect of degrading working conditions likely to infringe their rights and dignity, alter their physical or mental health or compromise their professional future") is prohibited and exposes the perpetrator to disciplinary and criminal sanctions.

Sexist and sexual violence covers all situations in which a person imposes on another person behaviour or statements (oral or written) of a sexist or sexual nature.
They can take a variety of forms: sexist offence, insult, sexual harassment, sexual assault, rape, etc.

Such violence violates fundamental rights, in particular the physical and psychological integrity of individuals. It is prohibited by law and punishable by law.

Anyone who is a victim of or witnesses hazing, bullying or sexual or gender-based violence may report it to the Rector, the ICT counselling unit or the Student Life Department.
With the consent of the witness or victim, the counselling team or the student life service can pass on the information to the victim.

report the situation to the ICT Rector for disciplinary action.

The Rector or Vice-Rector for Student Life and Academic Development may then decide :
- to launch an internal investigation;
- implement precautionary measures (such as a temporary ban on access to ICT campuses);
- initiate disciplinary proceedings that may result in permanent exclusion from the ICT campuses and from any public higher education institution with which the ICT has a partnership.
- to refer the matter to the Public Prosecutor, depending on the situation (article 40 of the Code of Criminal Procedure).

1.2. BEHAVIOUR AND RESPECT FOR PREMISES AND EQUIPMENT ENVIRONMENT

1.2.1. GENERAL RULES

The premises, including communal areas, green spaces and the area around the ICT, furniture and equipment of all kinds constitute the collective living and working environment for everyone and must be respected. It is therefore important to behave responsibly and to keep them in good condition and clean.

It is forbidden to bring pets onto ICT sites, with the exception of guide dogs on a lead accompanying people with disabilities, security guards or their trainer or host family.

Deliberate damage to the premises in the broadest sense of the term, or to the furniture or teaching materials made available by the ICT, in particular documentary, IT and audiovisual material, may result in disciplinary action up to and including permanent exclusion.

In addition, the act of tracing inscriptions, signs or drawings without authorisation is prohibited.

It is an offence punishable by law and liable to prosecution with a fine of up to €3,750 and community service.

1.2.2. THE TEACHING ENVIRONMENT

Everyone must be aware of and comply with the rules governing the use of the premises, in particular the computer rooms, shared workspaces and the university library.

In the event of authorised use or free access, the rooms must be restored if tables and/or chairs are moved.
No equipment may be moved to another room without authorisation.

In particular, learners should :

- Comply with the rules governing the use of the following facilities: classrooms, lecture theatres, computer rooms, common areas, shared work areas, museum area and university library;
- Keep the ICT premises and surroundings clean.
  For reasons of hygiene, it is forbidden to consume food or drink in the areas listed above. Only the rooms dedicated to catering must be used for this purpose (self-service or ICT Café area on the Fonderie site or Saint Dominique room on the Parlement site). Food waste must be disposed of in the bins provided and not in the waste paper bins in the offices and classrooms;
- Take care of the furniture and teaching equipment entrusted to them during their training: learners are required to use them in accordance with their purpose. Use for any other purpose is prohibited. At the end of the course, the learner is required to return all educational material and documents in its possession belonging to the ICT ;
- Respect copyright legislation and use the teaching materials provided during the course for personal use only.

<u>IT Charter</u>
When enrolling at the ICT, each student must read the IT charter in appendix 2 and undertake to respect its provisions.

Failure to comply with these clauses may result in the withdrawal of access to services, disciplinary action or criminal penalties in the event of a breach of the laws in force.

1.2.3. CATERING

Learners can only take their meals in the designated areas:

- Canteen (Fonderie site): learners have access to the canteen throughout the duration of the course, at the times shown.

The student card or the "carte étudiant des métiers" is compulsory in order to benefit from the ICT's contribution to the price of the meal. The card is topped up at the cash desk with a minimum amount set by the self-service manager. Bread, condiments, cutlery, trays, cups and the use of the microwave are reserved for the exclusive use of self-service customers. It is strictly forbidden to bring food from outside to eat in the self-service area.

- Café ICT (on the Fonderie site): learners can have their meals or snacks here. Food can be bought from the vending machines located there or brought in from outside. Rubbish

must be disposed of in the bins provided.

- Salle Saint Dominique (Parliament site): learners can also have their meals or snacks here. Food may be brought in from outside. Rubbish must be disposed of in the bins provided.

REMINDER: For reasons of hygiene, it is forbidden to eat in classrooms, lecture theatres, the university library, coworking spaces, the museum area, etc. and to throw food waste, cans and cups into the waste paper bins. You are asked to use the bins provided for this purpose and to practise selective sorting by using the systems set up for this purpose within the lCT to enable waste to be recycled and recovered.

It is also forbidden to throw rubbish on the public highway in front of the ICT.

1.2.4. PARKING

Within the lCT, two-wheelers must be parked in the spaces provided for this purpose, located solely in front of the museum area at 31, rue de la Fonderie and in the courtyard at 8 place du Parlement or, if necessary, in any other place communicated by the ICT Management. The courtyard of the Research Building is closed to the public.

1.2.5. RESPECT FOR THE ENVIRONMENT AND SUSTAINABLE DEVELOPMENT

In order to respect the environment, everyone must actively contribute to saving energy, fluids and consumables, whether in terms of copying documents, heating or lighting (close classroom windows after airing, do not block windows, etc.).

Make sure all non-automatic taps are turned off.

1.3 ICT'S LIABILITY IN THE EVENT OF THEFT OR DAMAGE TO LEARNERS' PERSONAL PROPERTY

The ICT accepts no responsibility for the loss, theft or damage of personal items of any kind left by students on its premises (lecture rooms, lecture theatres, administrative premises, car parks, courtyards, toilets, etc.).

SECTION 2: SPECIFIC RULES CONCERNING PREMISES

2.1. ACCESS TO SITES AND PREMISES

2.1.1 RESPECT FOR ICT OPENING HOURS

Access to the various ICT sites and premises is strictly reserved for learners, staff and other duly authorised visitors.
It is only possible during lCT opening periods and hours.
These are determined by the Rector and displayed at the reception of each site.
Outside these times, access to the various ICT sites is forbidden and learners are not allowed to remain on the premises after the sites have closed.

Special opening hours may be set for certain buildings, requiring appropriate security measures to be put in place.

Learners are also not permitted to remain in classrooms outside teacher attendance hours. A learner may not be given the keys to a room without the authorisation of the teacher in charge or the secretariat of the faculty, school or institute to which he or she belongs.

2.1.2 VIDEO PROTECTION AND ACCESS CONTROL

The ICT's teaching sites are under video protection and access control.
In accordance with French law no. 78-17 of 06 January 1978 on data processing, data files and individual liberties:

- Recorded images are only viewed by duly authorised persons. These recorded images are kept for a maximum of 30 days;
- Any interested party may request access to the recordings (video protection, access control) that concern them or verify their destruction within the time limits set. Such access is a right. Access may be refused on grounds relating to the rights of third parties.

All students enrolled at the ICT and all visitors must comply with the building access control system.

Access to the 3 ICT sites on the Toulouse campus is via :
- the student card or "carte étudiant des métiers", issued at the time of registration by the course secretariats; a new card will not be issued during the year, except in the event of loss or theft, and only on presentation of official proof (declaration of loss or theft), and on payment of €30;
- a temporary badge given to visitors at the reception desk of one of the 3 campus sites in exchange for a piece of identification.

Accessibility for people with disabilities is detailed in the inclusion and accessibility policy in appendix 3.

2.1.3 VIGIPIRATE PLAN AND SECURITY RULES

Safety is everyone's business. That's why it's important to adopt an approach based on monitoring, prevention, protection and safety.
The logo indicating the level of the Vigipirate plan is displayed at the entrance to ICT sites.

Depending on the level of the Vigipirate plan triggered by the Government, access to the premises may be restricted for reasons of safety and public order: filtering of entrances, visual checks of bags by security guards.
Refusal to undergo these checks may result in a ban on access to ICT sites.

Unusual attitudes or situations should be reported to the main reception, 31 rue de la Fonderie (05 61 36 81 00) :
- suspicious vehicle: prolonged parking, occupant behaviour, engine running ;
- attitude suggesting that they are on the lookout: coming and going, prolonged observation.

In the event of an alert, students must scrupulously comply with the evacuation or confinement instructions given by the school or the police.

2.2. PROVISION OF PREMISES

The provision of premises on a permanent basis to associations operating within the school is decided by the Rector of the LCT or his representative. This point is dealt with in section 3 paragraph 2 Freedom of association.

The occasional use of lCT premises, for any purpose whatsoever, for events or activities of any kind, at the request of organisers inside or outside the lCT, requires written authorisation from the Rector of the lCT or his representative, or the conclusion of an agreement. In all cases, the beneficiaries of the authorisation or the

The organisers must ensure that they comply with their regulatory obligations (declaration of the event to the prefecture, civil liability insurance, declaration of the opening of a temporary public house to the town hall, if applicable) and those relating to health and safety, particularly in terms of fire-fighting. They undertake to provide ICT with proof of their obligations.
In the event of non-transmission of documents, the ICT reserves the right to refuse to make its premises available.
This point is completed in section 3 paragraph 3 Freedom of assembly.

SECTION 3: USER RIGHTS AND FREEDOMS

3.1. POSTING AND DISTRIBUTION OF LEAFLETS (FREEDOM OF INFORMATION AND D'EXPRESSION)

Students at the lCT have the right to freedom of information and expression with regard to political, economic, social and cultural issues, and exercise this right individually and collectively (article L811-1 of the Education Code). The distribution and posting of leaflets, notices and press releases is free under certain conditions:

- All documents distributed must bear the author's signature and the identity of the printer. The author(s) assume full responsibility for the content of the posters and their display;
- The distribution of leaflets, notices and announcements by any person outside the lCT requires the prior authorisation of the Rector of the lCT;
- The ICT provides notice boards. Any posting of any kind whatsoever outside the reserved areas is prohibited and may result in disciplinary action being taken against the poster.

lCT staff are authorised to remove any posters that do not comply with current regulations.

The exercise of freedom of expression must not :

- Be likely to cause public disorder;
- To damage to respect the image of ICT;
- To damage to respect the environment ;
- Undermine the operation and character of the ICT.

3.2 FREEDOM OF ASSOCIATION

University associations of a scientific, social, sporting or cultural nature may only establish their headquarters at the ICT with the express authorisation of the ICT Rector. The request for authorisation must be made in advance and accompanied by the association's articles of association in force at the time the request is submitted. Only associations where the majority of the board members are enrolled in initial training or under an apprenticeship contract at the ICT are authorised to submit such a request. The ICT Rector must be notified of any subsequent changes to these rules.

Student associations based at the ICT undertake to send the Rector, via the Student Life Department, as soon as possible proof of the association's legal existence (extract from the JOAFE or receipt of the declaration from the Registrar of Associations), together with a certificate of civil liability insurance for the current academic year and the contact details of their legal representative.
They also undertake to submit an annual activity report to the Rector of the lCT. See appendix 5.

3.3 FREEDOM OF ASSEMBLY

No event or meeting outside the scope of the lCT's duties may be held or organised on the lCT's premises without prior authorisation from the ICT Rectorate and on the express condition that the mandatory security measures are implemented. II

The same applies when learners wish to invite outsiders onto the school's premises who have nothing to do with the lCT's activities.
There must be no possible confusion between the university and the organisers of the events, who remain responsible for the content of the speeches. It is the responsibility of the Rector of the lCT, with a view to giving or refusing his "prior agreement" to the provision of a room or site of the lCT, to take all necessary measures to ensure respect for freedoms within the establishment, to ensure the independence of the lCT from any political or ideological influence and to maintain order on its premises.

SECTION 4: DISCIPLINARY PROVISIONS

Disciplinary powers in respect of students are exercised by the Vice-Rector for Student Life and Academic Development on behalf of the Rector and, where appropriate, by the Disciplinary Board in initial education and the Disciplinary Committee in continuing education.
These bodies are made up of the Vice-Rector, the Dean of the Faculty or Director of the School or Institute or his/her representative, the Director of Studies to whom the learner reports, and a learner representative.

Pursuant to articles R811-10 et seq. of the Education Code, disciplinary proceedings may be instituted:

- Any fraud or attempted fraud committed during a test of knowledge and skills, whether as part of a continuous assessment or a final examination;
- Any fraud or attempted fraud in registration ;
- All productions that do not comply with the Intellectual Property Code (appendix 4);
- Any act likely to undermine the good order, proper functioning or reputation of the ICT, any failure to comply with the terms and conditions of the contract, or any breach of the terms and conditions of the contract.
- to these internal regulations and their appendices;
- Any failure to comply with the study regulations or examination charter of the faculty, school or institute to which the learner belongs.

The disciplinary penalties applicable to offenders are proportional to the seriousness of the offence committed and are as follows:
- WARNING;
- blame ;
- temporary exclusion for a maximum of five years or permanent exclusion from the ICT ;
- temporary exclusion for a maximum of five years or permanent exclusion from any public higher education establishment (decision taken by the Rectorat d'Académie or the public university awarding the degree).

Fines or other financial penalties are prohibited.

In the event of fraud or attempted fraud, the penalty incurred may, depending on the case, lead to cancellation of registration or invalidation of the test during which the fraud or attempted fraud occurred.

Any fact likely to trigger disciplinary proceedings must be reported in writing, with supporting documents, to the Dean of the Faculty or Director of the School or Institute.

The Dean or Director informs the ICT Vice-Rector for Student Life and Academic Development of the allegations made against the student.

Depending on the seriousness of the alleged offences and the proposed penalty, the Vice-Rector may or may not refer the case to the Disciplinary Board or Disciplinary Committee for review.

The Vice-Rector will inform the learner in writing of the grievances against him/her and of the possibility of

to consult their file. It also informs the employee of the penalties incurred.

If the investigation confirms the charges, and depending on their seriousness, the student is summoned by the Vice-Rector for Student Life and Academic Development or by his representative, by e-mail and by registered letter with acknowledgement of receipt or delivered to the person concerned against receipt, at least fifteen days before the date set, to attend a disciplinary board or committee meeting. The notice shall state the purpose of the meeting, the date, time and place of the meeting and whether the person concerned may be accompanied by a person of his or her choice.

At the Disciplinary Board or Committee meeting, the student is reminded of the reason for the proposed sanction. The student is then given the opportunity to give any explanation or justification for the acts of which he or she is accused.

When a protective measure of temporary exclusion with immediate effect is taken, no definitive sanction may be taken without the learner having first been informed of the grievances against him/her and having been summoned to appear before a Disciplinary Council or a Disciplinary Committee.
A student's absence from a disciplinary meeting is not grounds for postponing or cancelling the disciplinary session, except in cases of force majeure.

The Disciplinary Board or Disciplinary Committee will issue an opinion after hearing the learner.

The Vice-Rector for Student Life and Academic Development academic development, after consulting the Discipline Council or the Discipline Committee, will make a decision and inform the student.

Sanctions may not be imposed less than one clear day or more than 15 days after the interview or the opinion of the Disciplinary Board.

The learner is notified of the decision in writing, stating the reasons, by registered letter with acknowledgement of receipt or by hand-delivery against receipt.

Furthermore, in the event of a penalty being imposed on a trainee, the ICT management will inform :

- The employer of the trainee employee or the administration of the trainee employee when the training is commissioned by the employer or administration;
- The funder of the training course.

The decision may be appealed to the ICT Rector within 15 days of notification of the decision.

Disciplinary provisions for students enrolled in courses under agreement with a public university are governed by specific rules set out in the body of the School Rules or in the appendix thereto.

Disciplinary provisions for students in ecclesiastical faculties are subject to a specific regime set out in the faculties' statutes or in the ICT's canonical statutes.

SECTIONS SPECIFICALLY APPLICABLE TO CONTINUING EDUCATION TRAINEES AND STUDENTS UNDER APPRENTICESHIP AND PROFESSIONALISATION CONTRACTS

All the provisions of the previous sections of these internal regulations apply to continuing education trainees and students on apprenticeship and professional training contracts.
However, there are still a number of specific features that are independent of the headings presented above, and these are presented in this section.
The internal rules are drawn up in accordance with the provisions of articles L.6352-3 and L.6352- 4 and R.6352-1 to R.6352-15 of the French Labour Code. However, in accordance with article R.6352-1 of the

Code du travail, when the training takes place in a company or establishment that already has internal regulations, the health and safety measures applicable to trainees are those defined in these regulations.
Each trainee is deemed to have accepted the terms of these regulations throughout the duration of the training course and accepts that measures may be taken in the event of non-compliance.

SECTION 5: ORGANISATION OF TRAINING

5.1. TRAINING TIMETABLES

Trainees must comply with the timetables set and communicated in advance by the management either by means of posters, or when the training programme is handed out, or on the ICT's Scolaweb site. Failure to comply with these timetables may result in disciplinary action.

5.1.1. ABSENCES, LATE ARRIVALS OR EARLY DEPARTURES

In the event of absence, lateness or early departure, the trainee must inform the trainer or the ICT secretariat in charge of the training course and justify himself/herself to them. Furthermore, the trainee is not authorised to be absent during training hours, except in exceptional circumstances specified by the ICT management or its representative.
In accordance with article R6341-45 of the French Labour Code, trainees whose remuneration is paid by the public authorities are liable to have their training remuneration deducted in proportion to the duration of their absence. When the trainee is an employee undergoing training as part of the training plan, the ICT management will inform the company of such absences in advance. Any absence that is not justified by special circumstances constitutes misconduct liable to disciplinary action.

5.1.2. FORMALISM ATTACHED TO TRAINING FOLLOW-UP

All requests for remuneration or reimbursement of training-related costs, certificates of enrolment or entry into training must be submitted to the relevant departments as soon as possible.
It is compulsory for trainees to complete and sign the attendance sheet regularly as the course progresses. They may be asked to complete a training assessment. At the end of the training course, the ICT management will issue an end-of-training certificate and a certificate of attendance at the training course, to be sent to the trainee's employer or the organisation that financed the course, as appropriate.

5.1.3. INSTRUCTIONS IN THE EVENT OF AN ACCIDENT

Any accident or incident occurring on the occasion of or during training must be reported immediately to the ICT management by the learner or by those who witnessed the accident.
In accordance with article R 6342-3 of the French Labour Code, any accident occurring to a trainee while on the training site or while travelling to or from the training site shall be reported by the ICT management to the social security fund.

SECTION 6: TRAINEE REPRESENTATION

6.1. ORGANISATION OF ELECTIONS

When a training course attended by a trainee in continuing education lasts more than 500 hours, a full delegate and a substitute delegate are elected simultaneously in a two-round uninominal ballot. All trainees are eligible to vote. The ICT organises the ballot, which takes place during training hours, no earlier than 20 hours and no later than 40 hours after the start of the course.

If it is not possible to appoint trainees' representatives, the ICT will draw up a report on the failure to do so and send it to the regional prefect with territorial jurisdiction. The ICT management is responsible for organising the ballot. It ensures that the ballot runs smoothly.

6.2. TERM OF OFFICE OF TRAINEE DELEGATES

The delegates are elected for the duration of the training course. Their functions come to an end when they cease, for whatever reason, to participate in the training course. If the titular delegate and the alternate delegate have ceased their functions before the end of the training session, a new election is held under the conditions set out in articles R.6352-9 to R.6352-12 of the French Labour Code.

6.3. ROLE OF TRAINEE DELEGATES

The trainee delegates make any suggestions for improving the way training courses are run and the living conditions of trainees within the ICT. They present all individual or collective complaints relating to these matters, to health and safety conditions and to the application of the internal regulations. They are entitled to make known to the Advanced Training Council, where this is provided for, the observations of trainees on matters falling within the remit of this Council.

ENTRY INTO FORCE AND AMENDMENT OF THESE RULES OF PROCEDURE

These internal rules were adopted by the School Council on . . . . and will come into force on 01/09/2024.

These regulations may be amended at the initiative of the Vice-Rector for Student Life.

and Academic Development, Deans and Directors, Quality and Compliance. To be adopted, it must be presented to the School Council. Approval by at least the majority of members is required.

Toulouse, on: 19 June 2024

Professor François MOOG
Rector of the Institut Catholique de Toulouse

APPENDICES

Appendix 1: **Safety instructions**

Simplified fire instructions

1

You have witnessed a fire starting

2

Set off the alarm using a manual trigger

3

Call the fire brigade (0)18 on the landline or 112 on your mobile phone

4

Guide and control the evacuation by closing the doors behind you

5

Implement emergency measures to limit the development and spread of the fire

Never enter a premises without being visible

Evacuation

1

Lors d'un départ de feu, press the nearest alarm button. Without an indicator, the détecteurs de fumée déclenchent automatiquement l'alarme.

2

Dès que le signal d'alarme en suivant les guides d'évacuation et leurs instructions. sounds, drain into the water,

The evacuation guide is responsible for assembling and evacuating all the people following his training. He leads them to the assembly point.

3

Un serre-file s'assure que ne fait demi-tour. person ne reste en arrière or

In the absence of a guide d'évacuation:

1

Dirigez-vous vers les sorties de relief following the route sur les plans d'évacuation affichés à chaque étage et en vous aidant de l'éclairage de sécurité.

2

Rejoignez le point de

votre site :

designated for

- ↳ **Site de la Fonderie**
- Cours supérieure
- ↳ **Site du Parlement**
- Place du Salin
- ↳ **Sites des Fleurs**

Rue des fleurs

dans lequel vous vous trouvez.

To reach rassemblement:

- Do not use lifts. Never go
- backwards.
- If the smoke is large, ne tentez pas de les affronter, baissez-vous (au sol, la visibilité et l'air sont meilleurs).
- Wait authorisation from réintégrer les locaux.

Important: Remain at rassemblement durant toute l'alerte jusqu'à la fin de l'alerte annoncée par le responsable d'évacuation.

Meeting point

Instructions in the event of illness or accident

Before any intervention, and in order to avoid an "accident on top of an accident", all sources of danger must be removed. To do this, you need to protect yourself, the victim and anyone else in the vicinity.

Then, as a priority, contact :

Internal emergency services

- First aiders at work (SST)
- If you can't find a workplace first aider, contact reception (05.61.36.81.00).

OR

External emergency services

- Fire brigade (18)
- SAMU (15)
- Zones without network and European call number (112)
- For the hearing impaired(114)

The Management contact person in the event of illness or accident: Chrystel Bodoira (06.30.50.40.94)

The Alert Message

Sound the alert using a portable telephone or, failing that, a landline telephone. Specify in the alert message :

- Youridentityand call number
- The precise location of the accident: address, workshop, floor, etc.
- The nature of the accident: a fall down a flight of stairs, feeling unwell in class, etc.
- The number of victims
- The condition of the victim(s)
- Actions already underway

To ensure that the message is properly transmitted:

- Answering questions asked by the emergency services
- Never pick up the first
- If a call is made by a third party, they will be asked to report to the OHS.
- If possible, send a person to meet the victim.

In all cases, follow the instructions given by the emergency services and organise their

access to the accident site, as close as possible to the victim.

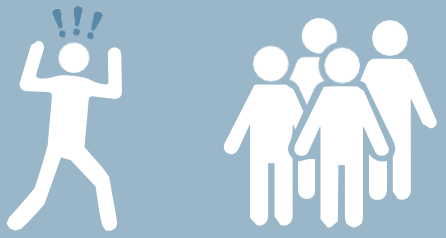
Vigipirate instructions

1 Escape

Locate the danger so you can get away

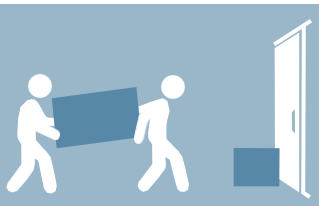
If possible, help others to escape

Do not expose



Alert people around you and discourage them from entering the danger zone

2 Hide



Lock yourself in and barricade

Turn off the light and mute any equipment

Move away from openings and lie down on the floor.

Otherwise, take cover behind a solid obstacle (wall, pillar, etc.).

In all cases, turn off your phone's ringer and buzzer

3 Alert

As soon as you are safe, call 17 or 112

Do not run to the forces of law and order and do not make any sudden movements.

Keep your hands up and open

If you witness a **suspicious** situation or **behaviour**, contact the police (17 or 112). When you enter a premises, look out for the **emergency exits.** Do not spread any information about the intervention of the police. Do not spread rumours or **unverified information** on the Internet or social networks. On social networks, follow the **@PlaceBeauvau** and **@gouvernementfr** accounts.

Appendix 2: Charter for the use of ICT information systems

The present charter is a legal document which defines the rules of use and security which the Institut Catholique de Toulouse (ICT) and the user undertake to respect when using internal IT services and resources: it specifies the rights and duties of each party. It also aims to make users aware of the risks associated with the use of these resources in terms of the integrity and confidentiality of the information processed.

Preamble

Information and digital systems (SIN) cover all the hardware, software, applications, databases and telecommunications networks that can be made available by the Institut Catholique de Toulouse (ICT):
- Electronic mail ;
- Software ;
- Servers ;
- ERP ;
- Internet ;
- Social networks ;
- Collaborative work and service platforms: Microsoft Teams, Moodle, etc.

Mobile computing, such as laptops and mobile phones allocated to staff authorised by the establishment and supplied by the ICT, are also components of the INS.

The term "user" refers to any person who has access to the resources of the INS as part of their professional or educational activity, regardless of their status.
These include :

- Any external staff or service providers involved in carrying out its administrative and/or teaching duties;
- All students enrolled at the ICT or renting accommodation in one of the residences on the ICT campus;
- All ICT alumni for e-mail only;
- Any staff invited by the ICT as part of research, teaching or administrative cooperation.

I. Fields of application

The rules of good IT practice and security, set out in this IT charter, apply to anyone wishing to connect to the ICT IT network, either on site or remotely.

The proper operation of the Information and Digital Systems Service (SSIN) requires users to comply with all applicable laws and regulations (see list below, which is not exhaustive):

I.1/ Applicable regulations

- Regulations relating to public order, public decency and personal rights: the following in particular are prohibited: content of a violent, defamatory, insulting, racist, pornographic or illegal nature that is likely to harm the integrity or sensitivity of another person;
- Regulations relating to respect for the privacy of individuals (article R226-1 of the French Penal Code and article 9 of the French Civil Code): content infringing on the right to a person's image, the right to privacy, defamatory or insulting content is prohibited;
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of individuals with regard to the processing of personal data and on the free movement of

and repealing Directive 95/46/EC (General Data Protection Regulation). Any violation exposes the perpetrator to disciplinary and criminal sanctions in accordance with the regulations in force, in particular with regard to articles 226-13 and 226-16 to 226-24 of the French Criminal Code;

- Copyright regulations (Intellectual Property Code);
- In any event, users are subject to the obligations resulting from their status or contract;
- Regulations governing computer fraud (articles 323-1 et seq. of the Criminal Code).

I.2/ ICT commitments

The ICT informs users of this charter when they arrive at the ICT. It is also appended to the internal rules for staff and the internal rules for students, which makes it binding.

The user hereby undertakes à respect its provisions.

The ICT facilitates user access to INS resources and implements all necessary measures to ensure the security of the INS and the protection of users:

- Limits access to only those resources for which the user is expressly authorised;
- Regularly communicates the rules of good IT practice to users by e-mail and updates this IT charter;
- Respect employees' right to disconnect.

I.3/ The user's commitments

Users are responsible at all times for the use they make of the ICT INS to which they have access. The user accepts this charter fully and without reservation and undertakes to comply with it throughout the period of use of the INS.

II. Rules for using INS

II.1/ User access conditions

Logical access control makes it possible to identify anyone using a computer.
The following information is provided:
- administrative identification (login + password) for each employee with an administrative role;
- and/or a pedagogical identification for each user with a pedagogical activity and for each learner registered with the ICT.

Identification is a security measure designed to prevent malicious or abusive use. Each time a user logs on, they are assigned their own rights to the INS resources they need for their activity. This access right is therefore strictly personal and non-transferable.
It ceases when the user leaves the ICT or if it is established that the user has violated one of the obligations of this charter.
The right of access is granted to the user solely for the purposes of use compatible with the activities of the ICT, whether administrative, educational or research. It excludes any other use, in particular commercial use.
The user acknowledges that he/she may be held liable for the use of his/her access rights under the conditions set out in this charter.
Any violation of the conditions of access described in the charter, in addition to disciplinary sanctions, may give rise to civil liability on the part of the perpetrator and constitute an offence within the meaning of articles 323-1 to 323-7 of the French Penal Code.

II.2/ Personal data protection policy

II.2.1 / Protection of INS users

- Use of the INS may require the communication of personal data. Personal data means

  personal data: any data that directly or indirectly identifies an individual, in any form whatsoever.

The ICT complies with French law no. 78-17 of 6 January 1978 as amended, known as the "Data Protection Act", and with European regulation no. 76-679 of 27 April 2016, known as the RGPD.
The purpose of collecting and processing personal data is to :

- Create a directory of user accounts to enable access to IT resources made available on the ICT's wired and wireless networks;
- Enable authenticated access to IT resources and services implemented on the ICT IT network;
- Comply with regulations, in particular for detecting and combating criminal offences, when circulating data on the Internet, in particular e-mail or web browsing;
- Ensure the storage and/or archiving of sensitive files/emails/research data that the user wishes to keep only on professional media approved by the ICT's SSIN.

In accordance with these provisions, all users of the INS have the right to access, rectify, limit and delete, as far as possible, all data relating to them, including data relating to the use of the INS.
These rights may be exercised by contacting the Data Protection Officer at dpo@ict- toulouse.fr, and a complaint may be made to the CNIL (French Data Protection Authority).

possible for users if they consider that their rights have not been respected.

II.2.2 / Compliance with data protection regulations by INS users

Users of the INS are hereby informed of the need to comply with the legal provisions relating to the automated processing of personal data, in accordance with Act No. 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties, as amended by Act No. 2004-801 of 6 August 2004, and with the directives of the RGPD.

- Any creation of files containing this type of information and requests for related processing, including when they result from the cross-referencing or interconnection of pre-existing files, are subject to the prior formalities provided for by law.
  "Informatique et Libertés" and the Regulation (RGPD);
- Consequently, any user of the INS wishing to proceed with such a creation must first inform the relevant departments, in particular the Data Protection Officer (DPO), at the following e-mail address: dpo@ict-toulouse.fr. The DPO will take the necessary measures to ensure compliance with legal provisions.

The ICT, in accordance with its legal obligation under Article 5 of the RGPD, has set up a system for logging Internet access, email and data exchanged in order to detect incidents, intrusions and unauthorised use or misappropriation of computer systems by users.
The ICT reserves the right to set up, if necessary, traceability tools on all information systems. Prior to this implementation, the ICT will notify the staff representative bodies and will make a declaration on its data processing register.

CNIL, which will mention in particular the length of time for which traces and connection times will be kept, and the conditions of the right of access available to users, pursuant to law no. 78-17 of 6 January 1978, amended by law no. 2004-801 of 8 August 2004.

II.3/ Best practice rules for workstation safety at the ICT

Whatever the device, the user must exercise caution and follow good practice when using the workstation. They must not :

- Accessing or attempting to access INS resources for which they have not received explicit authorisation: the levels of access available to the user are defined according to the mission entrusted to them;
- Connecting equipment directly to the local networks other than that entrusted or authorised by the ICT. Any connection of personal equipment to the ICT's local networks poses a risk, as their level of security is neither controlled nor verifiable;
- Be alert to phishing attempts;
- Do not use your ICT professional login for personal purposes;
- Install, download or use on ICT equipment, software or software packages for which licence fees have not been paid, or which do not come from reputable sites, or without authorisation from the INS;
- Directly or indirectly disrupt the operation of the network and the INS to which it has access and cause modifications, alterations or destruction of data or files other than those of its own creation;
- Reproduce, copy, distribute, modify or use the software, databases, web pages, texts, images, photographs or other creations protected by copyright or any other intellectual property right.

private right, without having obtained prior authorisation from the holders of these rights ;

- Copying works protected by copyright.

The user undertakes to :

- Respect the rules of confidentiality with regard to the information and documents to which it has access. This obligation implies compliance with the rules of professional ethics and deontology;
- Install only the applications you need, and always with SSIN authorisation;
- Make regular back-ups on the ICT network;
- Comply with the measures put in place by the ICT to combat viruses and attacks by computer programs;
- Report any malicious act or suspicion of malicious act observed on the devices used, whether professional or personal, if there has been a connection to the network or to an ICT online service.

II.4/ ICT's policy for authenticating and managing access to user accounts

II.4.1 / General policy

Unique identification is a security measure designed to prevent malicious or abusive use. Each time a user logs on, they are given their own rights to the INS resources they need for their activity (administrative and/or educational).

- Each password must be changed at the following intervals: every 6 months ;
- To be effective, a password must contain at least 12 alphanumeric characters of 4 different types, including at least uppercase, lowercase and uppercase letters.

numbers and special characters.

- It must not :
  - Be identical to the login, even if the characters are reversed;
  - Include information about the user (surname, first name, telephone number, date of birth, etc.);
  - Be a word or a list of words in the dictionary or a proper noun, place name ;
  - Be saved on a single file but in the application "KEEPASS" installed on ICT computers;
  - be communicated to a third party: login and password are strictly confidential. The user is personally responsible for any use that may be made of it, and must not at any time disclose it.
- Users must respect access management, and in particular must not use another user's login or password, or try to find out about them.

If, for exceptional and specific reasons, a user is obliged to give his/her password, he/she must change it as soon as possible or request a change from the administrator.

- Users should use unique passwords for each service, site and software used. It is recommended not to use a password that has already been used for a personal tool. Using the same password for all sites only increases the IT risk.

II.4.2 / Teleworking policy

For security reasons, employees eligible for teleworking are not allowed to work remotely, is only possible under the following conditions:

- Connection only from a computer made available by the ICT, protected by a virtual private network (VPN), to carry out its professional activity;
- Double authentication for connection via the Fortitoken application, to be installed on the teleworking user's personal telephone, in order to receive the authentication code;
- Applying security updates to all professional equipment as soon as they are made available (PCs).

The use of personal tools for professional purposes is not recommended.

II.5/ Rules governing the use of electronic mail

The use of email is one of the key ways of optimising work, sharing and exchanging information within the ICT.
The ICT provides users with a nominative or shared professional mailbox, enabling them to send and receive electronic messages, which may only be used for professional purposes.
The management of e-mail addresses corresponding to institutional mailing lists, designating a category or group of users, is the sole responsibility of the ICT: these addresses may not be used without explicit authorisation.

E-mails and attachments play a major role in computer fraud. Users should be particularly vigilant when using their work email and be wary of phishing attempts. These techniques consist of a hacker sending a fraudulent e-mail to encourage the recipient of the message to divulge their personal data.

personal information, for example by pretending to be a well-known organisation or third party.
The user must :

- Check the sender of the e-mail and if in doubt alert the ICT IT department support@ict-toulouse.fr
- Do not open e-mails or attachments from unknown or suspicious senders;
- Protect your digital identity to limit the risk of fraud.

Furthermore, in accordance with the penal code, users must not disseminate information or data of an illegal nature, particularly racist, defamatory or insulting. Consultation of sites with pornographic content from ICT premises is prohibited.

II.5.1 / Secure data sharing

A message sent via the Internet (email, Teams, ...) can potentially be intercepted, even illegally, and read by anyone.

It is forbidden to use unsecured sites for sharing large amounts of data, such as We Transfer, Dropbox or others.
Only the use of FILESENDER managed by GIP RENATER, the file transfer service of the Higher Education and Research community, is authorised for sending large files or files containing sensitive or confidential data, as it allows data encryption. It provides temporary storage space for ICT staff and their privileged contacts. It guarantees :

- Authentication via the Education-Research identity federation to which the ICT is referenced;
- A temporary file repository (up to 100 files for a maximum repository size of 100 GB; size maximum file size for non-HTML.5 browsers: 2 GB ;
- deposit expiry date: maximum 30 days), to one or more correspondents (up to 50 e-mail addresses separated by a comma or semicolon);
- End-to-end encryption certified by ANSSI ;
- View and download the files submitted;
- An invitation from correspondents, whether in France or abroad, to upload files to their personal file upload space (invitations expire after a maximum of 30 days).

II.5.2 / Private use of e-mail

The residual use of e-mail for private purposes is tolerated if it is non-profit-making and reasonable in terms of frequency, volume and duration.
Such use must not adversely affect the quality of the user's work, the time he or she spends on it or the smooth running of the service.
All messages in the mailbox are deemed to be professional, with the exception of those explicitly designated by the user as being of a private nature. It is the user's responsibility to mention the private nature of a message in the subject line and to store it in a directory identified as being of a private nature, using the keywords PRIVATE or PERSONAL.
Users are responsible for regularly saving private messages.

II.5.3 / Consultation of the e-mail account by the ICT

"Files created, sent or received from the workstation made available by the employer are in principle of a professional nature".

Thus, the ICT may consult, even when the employee is not present, any electronic mail received or sent by the latter from his or her professional mailbox. On the other hand, the ICT is prohibited from consulting, even in the presence of the employee, messages marked "Personal" or "Private" or stored in a directory marked as such.
There is, however, one exception to this protection: if the ICT can justify "special circumstances" enabling it to seek judicial authorisation to access the employee's personal or private e-mails, or if a judicial investigation is underway.

ICT's right to consult the employee's mailbox and continuity of service

Continuity of service and prolonged absence
In the event of prolonged absence (holiday, illness, precautionary lay-off, etc.): if the absent employee holds information on his workstation that is essential to the continued operation of the department, the ICT may demand that the employee's login and password be communicated, if the network administrator is unable to provide access to the employee's workstation *(CNIL/control of internet and e-mail use*).
In this case, all messages, except those identified as personal or private, will be retrieved by the person responsible.
An automatic message can be sent from the employee's mailbox giving the names of people to contact in the employee's absence, thus ensuring continuity of service.

Continuity of service and employee departure
In the event of an employee's definitive and scheduled departure (resignation, contractual termination, redundancy with notice period, retirement, etc.), the employee's access, including remote access to his or her email account, is deactivated the day after the last day of the employee's notice, even if the notice period has not been served.

Employees must empty their professional email account of any email/folders identified as personal or private before their departure date.

The closing date of the employee's e-mail account is set at the last day of the employee's contract + 6 months for reasons of continuity of service.
At the decision of the line manager, messages are forwarded to the department's address or a nominative address during these 6 months to ensure continuity of service.
At the end of this period, the employee's personal e-mail address is deleted.

In the event of an unscheduled departure, the employee will be informed by his N+1 of the date on which his mailbox will be closed within a reasonable period of time, so that he can make arrangements and retrieve only those messages identified as personal or private, under the supervision of a trusted third party.
The mailbox must be permanently closed on the date indicated by the N+1.

Precautionary dismissal and suspension of an employee's access to his work e-mail account
In the event of a precautionary layoff (a preventive, immediate and temporary measure taken by the employer in the event of a serious breach committed by the employee making his presence at the ICT impossible, while a decision is taken on the employee's fate), the employee's access to his professional email will be suspended by the ICT for the duration of the employee's precautionary layoff.

E-mail retention

Type of e-mail	Shelf life	Legal or regulatory basis
Personnel management e-mails	Up to 5 years after the end of the contract	French Labour Code
Commercial e-mails	3 years minimum	Accounting and tax obligations
Tax e-mails	6 to 10 years	Accounting and tax obligations
E-mails containing personal data	Necessary duration according to purpose	RGPD
E-mails relating to employment contracts	The entire term of the contract + 5 years	French Labour Code
E-mails concerning disputes	Up to resolution + 5 years	Legal precautions
Correspondence linked to specific projects	Project duration + 3 years	Project management
Training and professional development e-mails	2 years after last use	Human resources management
Health-related e-mails and safety at work	Entire period of employment + 5 years	Labour Code, RGPD
E-mails relating to customer complaints	5 years after the resolution	Customer management, RGP D
Important internal correspondence	Indefinitely or according to internal policy	Management company
E-mails linked to internal investigations	At least 5 years after the end of the survey	RGPD, employment law
E-mails concerning rights copyright and intellectual	Up to 70 years after the death of the author	Copyright, intellectual property
E-mails relating to controls and audits	10 years	Financial and accounting regulations
E-mails containing annual financial information	At least 10 years	Accounting and tax obligations
E-mails relating to insurance and insurance policies	Policy term + 10 years	Insurance law

II.6. Rules for using the Internet

You are reminded that the Internet is subject to all the legal rules in force, a list of which is given in paragraph I.1 p.3.

The use of the Internet is an essential element in optimising work, pooling information and making it more accessible both within and outside ICT.
The ICT provides users with Internet access whenever possible. The Internet is a working tool open to professional use (administrative and educational).

Safety :

- Users must check the security of the sites they visit and give preference to official sites and sites whose address begins with "https://".
- The ICT reserves the right to filter or prohibit access to certain sites, and to carry out a priori or a posteriori checks on the sites visited and the corresponding access times.

II.7. Rules for using social networks

It should be noted that the use of social networks is subject to all the legal rules in force, a list of which is given in paragraph I.1 p.3.

Disclosing confidential information via social networks, publishing images of the company or its members without prior authorisation, or making comments about ICT or its members that go beyond the scope of freedom of expression may result in disciplinary or even criminal sanctions.

Any comments made on a social network are the responsibility of the author and do not constitute an official statement by ICT.

In addition, if a user is contacted via a social network, they should check the identity of the person requesting the information: as with phishing, requests for personal information can be made via social networks, by people who may refer to emergency situations, requests for confirmation, and so on.

III. INS safety rules

III.1 Reporting and information duties

Users must notify the SSIN as soon as possible of any malfunction or anomaly discovered in the information system.

III.2 Control and safety measures

The SSIN ensures the smooth running and security of the ICT's networks, IT resources and communications. The members of this department have the technical tools they need to carry out investigations and monitoring the use of IT systems set up in compliance with applicable legislation.
Staff responsible for controlling information systems are bound by professional secrecy. They may not divulge information that comes to their knowledge in the course of their duties if :

- this information is covered by the secrecy of correspondence or is identified as such and is part of the user's private life;
- they do not jeopardise the proper technical operation of the applications or their security, they do not fall within the scope of article 40 paragraph 2 of the Code of Criminal Procedure.

III.2.1 Procedure in the event of cyber-malware

Phishing is a fraudulent text message or e-mail designed to trick the victim into providing personal and/or banking data (access accounts, passwords, etc.) by pretending to be a trusted third party.

1. <u>The rules of good IT practice against a *phishing* attempt</u> :

- **1. Never communicate sensitive information by e-mail or telephone:** No administration or company will ask you for your bank details or passwords by e-mail or telephone.

- **2. Before clicking on a dubious link,** position the mouse cursor over the link (without clicking), which will then display the address to which it actually points in order to check its plausibility, or go directly to the site of the organisation in question via a favourite link that you have created yourself.

- **3. Check the address of the site displayed in your browser.** If it does not correspond exactly to the site in question, it is almost certainly a fraudulent site. Sometimes a single character in the site address can change to mislead the user. If in doubt, do not provide any information and close the corresponding page immediately.

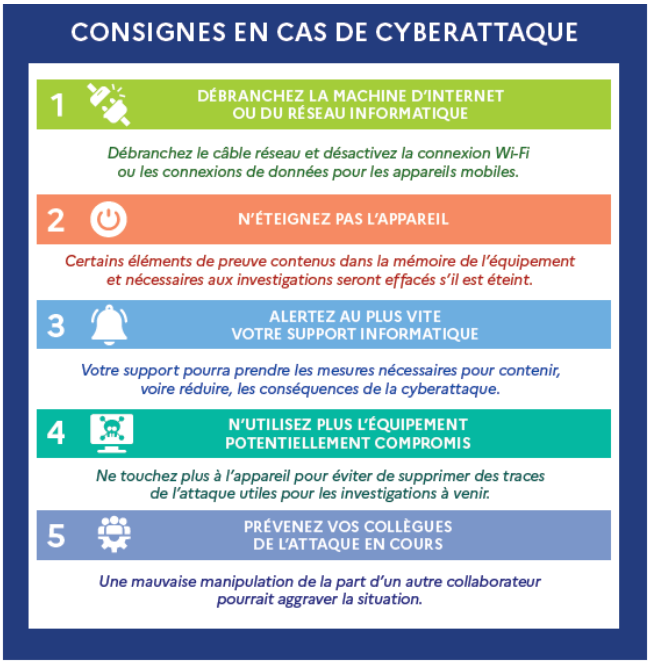
- **4. If in doubt, contact the NSSI immediately.**

- **5. Use different, complex passwords** for each site and application, to prevent the theft of one password from compromising all your accounts.

- **6. If the site allows, check the date and time of the last connection to your account in** order to identify any illegitimate accesses.

- **7. If the site allows, activate double authentication to secure your access.**

III.2.3 Procedure in the event of a cyber attack



Pour vous informer sur les bonnes pratiques
et les principales menaces en matière de cybersécurité
rendez-vous sur :
www.cybermalveillance.gouv.fr

IV. Limiting use

In the event of non-compliance with the rules set out in this charter, and without prejudice to prosecution or criminal sanctions, it may be decided to take measures to limit use, as a precautionary measure, and to impose disciplinary sanctions.

V. Entry into force of the charter

This charter is appended to the ICT's internal regulations, which were approved by the ICT's Board of Directors on 15/05/2024.

Toulouse, 19 June 2024

Professor François Moog
Rector of the Institut Catholique de Toulouse

Annex 3: Inclusion and accessibility policy

STUDYING A T ICT WITH DISABILITIES: OUR INCLUSION POLICY

The aim is to develop an inclusive quality approach in order to guarantee all learners from initial training or vocational training who have a disability, accessibility in all its dimensions within the ICT (accessibility to premises, access to information, knowledge, student life, studies, the Skills Centre, the Library, International Relations, the Cultural Centre, etc.). Learners with disabilities must benefit from all the mainstream services provided by the ICT.

The issue of inclusion is an integral part of the school's CSR policy, and the disability dimension - whether visible or less visible - is of particular importance. The first step is to set up and improve systems for welcoming, supporting and providing feedback to students with disabilities. This is backed up by the development of partnerships with external entities (service providers, companies, associations, local authorities) to create a network that can be mobilised.

The ICT's Mission handicap is organised in accordance with the legislative framework: the law of 11 February 2005, circular no. 2011-220 of 27 December 2011: Examinations and competitions in school and higher education and the Charte université handicap of 19 April 2012.

WELCOMING AND PROVIDING SUPPORT: THE ROLE OF THE MISSION ACCUEIL HANDICAP

As the interface between students with disabilities and the various players in the institution (administrative and teaching teams), the role of the Mission Accueil Handicap is to supervise and ensure compliance with the adjustments recommended by the Service Interuniversitaire de Médecine Préventive et de Promotion de la Santé (SIMMPS) so that students can follow their course of study in the best possible conditions.

A MISSION OF WELCOME

At the beginning of the academic year, a study of the specific needs of learners (continuing education and vocational students) with disabilities is carried out, following a prior visit to the Preventive Medicine Department. We then put in place appropriate monitoring and accommodation, in conjunction with the various players and partners: teaching and administrative teams, the Interuniversity Preventive Medicine and Health Promotion Service (SIMPPS), the Skills Centre and external partners.

A liaison form reflecting the SIMPSS notification will then be issued for validation of the ICT learner's MAH protocol. It is essential to make these contacts as soon as possible so that you can benefit from the adjustments as soon as the new school year starts.

Support measures are adjusted according to changes in the learner's state of health and/or the emergence of new training-related needs.

SOME EXAMPLES O F LAYOUTS POSSIBLE (non-exhaustive list)

- Additional test time ;
- Educational support (tutoring) ;
- Note taker (learner helper) ;
- Go to à available of equipment (computer, software, etc.) ;
- Adaptations of documents (enlargement, etc.) ;
- Curricular adjustments ;
- Suitable media;
- Break time ;
- Separate or small rooms;
- Exam secretariat ;
- Free photocopies.

A MISSION OF SUPPORT

We offer a number of schemes, as well as a network of administrative and teaching teams through the network of disability liaison officers (CRH), who are the main contacts within faculties and organisations. We also work with external partners in a mobilisable network.

In order to optimise the implementation and monitoring of these arrangements, we insist throughout the year on awareness-raising initiatives aimed at the entire ICT community (learners and teams), as well as specific training for administrative and teaching staff. Quality is monitored by means of satisfaction questionnaires, so that any necessary adjustments can be made.

EXISTING FACILITIES (non-exhaustive list)

- Specialist educator for learners with autism ;
- Psychological helpline ;
- Workshops on stress management, concentration, etc.
- Theme-based awareness campaigns.

Supporting students with disabilities is an essential part of our institution's mission. The ICT wants to ensure that disabled students have access to all aspects of university life, and reminds them that welcoming disabled students is everyone's business.

ACCESS AND BROWSE : AN ACCESSIBLE UNIVERSITY

In this place steeped in history, the Institut Catholique de Toulouse's accessibility and inclusion policy aims to take accessibility into account as a fundamental element of a campus adapted to its learners.

ACCESSIBILITY OF PREMISES

In compliance with current standards, the ICT premises are accessible to people with reduced mobility. The lifts, evacuation chairs and flashing lights (in the toilets in particular) are regularly inspected.

Accessibility registers are available for consultation at the reception desks of all three sites.

Important: as our establishment is currently undergoing a period of renovation work, we have received approval for a programmed accessibility schedule.

DIGITAL ACCESSIBILITY

Numerous computers are available, particularly in the coworking areas, during the school's opening hours. A fleet of laptops is also available for students to use when writing their continuous assessment tests and/or mid-term exams, or to get to grips with the digital world.

Consideration has been given to a request for approval for the ICT university library to use the PLATON platform.

Annex 4: Intellectual property and fraud

The use of the documentary resources (digital resources, paper, etc.) implies respect for the intellectual property rights of the author as well as those of his partners and, more generally, of all third parties holding such rights.
Consequently, each user must :

- Use the software in accordance with the terms of the licences purchased;
- Not to reproduce, copy, distribute, modify or use software, databases, documents from Internet pages, texts, images, photographs or other creations protected by copyright or a private right, without having obtained the prior authorisation of the holders of these rights.

Any oral or written work submitted by a learner must represent their own efforts or those of their group.
Fraud is therefore committed if the learner or their group exploits the work of others or produces content using a generative artificial intelligence tool (e.g. ChatGPT) as if it were their own work. It is particularly forbidden to :

- Use the exact terms of a publication without quoting it in inverted commas and clearly identify the source (in a footnote, for example);
- Paraphrasing or reformulating a concept, research or interpreting ideas (verbal or written) of another legal or natural person, without quoting them and identifying the source, whether free of charge or in return for payment;
- Present research data that has been falsified or invented in any way whatsoever;
- Presenting the same work or a significant part of the same work in more than one course, or another work already presented elsewhere, without the prior written permission of the teachers concerned;
- Falsifying or distorting an academic assessment ;
- Using a document that has been forged or falsified in order to divert it from its normal use;
- Copy the data produced by a generative artificial intelligence tool (e.g. ChatGPT) without quoting the tool used or the transcription of the content generated by the AI.

Group work is subject to the same rules of intellectual integrity as individual work. In the event of non-compliance with ethical rules, the group is considered to be jointly and severally liable to fraud. It may be penalised.

The ICT is equipped with software to detect similarities and content generated by generative AI, Compilatio (https://www.compilatio.net/). This tool searches for and quantifies (as a percentage of similarities) similarities in the document analysed with source documents (internet pages, scientific publications, documents added by ICT teachers) and content produced by generative artificial intelligence.

Interpretation of the results and study of similar passages is at the discretion of the marking teacher.

Appendix 5: Student associations and student life

GENERAL PRINCIPLES

Learning associations carry out their activities in conditions that do not interfere with teaching and research activities and that do not disturb public order. All activities that violate the lCT charter are prohibited. Commercial activities may only take place with the authorisation of the lCT's management and in compliance with the association's articles of association and the regulations in force, particularly those relating to taxation and accounting. Activities that contravene IT laws are prohibited. Learner associations are responsible for the premises and equipment made available to them. As a general rule, the lCT reserves the right to suspend any event, particularly in the event of public order disturbances, health and safety violations or endangerment of persons.

PRINCIPLES OF RECOGNITION OF STUDENT ASSOCIATIONS BY I'ICT

Associations may apply for recognition if their main activities are carried out at the ICT, their projects have an impact on learners at the ICT and the majority of their officers are ICT learners.

PROCEDURE OF RECOGNITION OF STUDENT ASSOCIATIONS BY ICT

Associations wishing to obtain recognition must be legally associations under the 1901 law that comply with legal obligations and whose articles of association have been filed with the prefecture. The association then submits a copy of these documents, together with a copy of the receipt issued by the prefecture, to the ICT Student Life Department and the ICT Rectorate. The association must also provide proof that it has taken out civil liability insurance covering its statutory missions. The BVE (with the help of the General Secretary, the Vice-Rector for Student Life and Academic Development and the Director of the ICT Rectorate) is responsible for registering the association.

de la communication) verifies whether the association's purpose complies with the general principles of recognition.

The Vice-Rector for Student Life and Academic Development is then informed and submits approval of the recognition to the ICT Rector. The CVU (University Life Council) is informed once a year of the list of learning associations receiving recognition.

DURATION AND RENEWAL OF RECOGNITION

Recognition is granted for one academic year. Associations must renew their application each year before 15 November. The BVE and the Vice-Rector for Student Life and Academic Development must be notified without delay of any changes to the association's articles of association, the composition of its executive committee or its dissolution. Each year, at the latest at the time of the application for renewal, the association must submit to the Vice-Rector for Student Life and Academic Development a written report on the activities carried out during the previous year, as well as a financial report, and provide proof of insurance valid for the whole of the current academic year.

ASSOCIATIONS REGISTERED WITH ICT

Recognised associations may apply to be registered at the ICT. The request is sent to the Vice-Rector for Student Life and Academic Development and approved by the Rector of the lCT. Authorisation to use the ICT as a registered office does not imply the allocation of premises.

PROVISION OF PREMISES

LCT premises can also be made available on a more regular basis for the day-to-day activities of associations. These premises are allocated as a priority to associations that regularly contribute to the activities of the university community. Premises may be made available to

These facilities are available to learner associations on a one-off basis for a specific project (conferences, various meetings, information stands, cultural or sporting events, etc.).

TEMPORARY PROVISION OF PREMISES

Associations may ask to reserve lCT premises for their specific activities during the school's opening hours. A request for a reservation setting out the purpose of the activity must be sent to the Student Life Office (BVE). No student event may take place without written agreement. The minimum deadline for submitting a request is 15 days before the date of the planned event.

STUDENT INVOLVEMENT

In accordance with decree no. 2017-962 of 10 May 2017 on the recognition of students' commitment to community, social or professional life, learners have the opportunity to value community, social or professional activities mentioned in article L. 611- 9 of the Education Code: "voluntary activity within an association governed by the law of 1st July 1901 relating to the contract of association or entered in the register of associations pursuant to the local civil code applicable in the departments of Bas-Rhin, Haut-Rhin and Moselle, professional activity, military activity in the operational reserve provided for in Title ll of Book ll of Part IV of the Defence Code, volunteer fire-fighter commitment provided for in article L. 723-3 of the Internal Security Code, civic service as provided for in II of article L. 120-1 of the National Service Code or voluntary service in the armed forces as provided for in article L. 121-1 of the same code
".

In addition, there are the following activities: community involvement and voluntary work, student involvement activities (student associations), involvement in lCT cultural projects, professional initiative projects, etc. A bonus system will be introduced to reward these activities.

in place, guaranteeing validation of the skills, knowledge and aptitudes acquired by their learners in order to obtain a diploma. To benefit from a bonus, the student must submit the Student Commitment validation request for approval by a committee before the date defined each year. At the end of the academic year (depending on the date set each year), the student must submit a duly completed Dossier Personnel d'Engagement Étudiant (DPEE). Validation of the Student Commitment is recorded in the descriptive annex to the diploma.

EXCEPTIONAL SALES AND VARIOUS PROMOTIONAL OPERATIONS

The associations respect the lCT's principle of commercial neutrality. The sale of products on university premises by students must be exceptional and directly linked to a student activity. They may be authorised from time to time to organise small-scale commercial events (breakfasts, cake sales, tombolas, etc.) in or in front of teaching buildings. However, these are limited to 5 events per year and per association. The association must apply to the BVE at least 15 days before the planned date(s). The decision is confirmed by a letter of authorisation setting out the conditions under which these activities may be carried out.

POSTER SPACE AND LEAFLET DISTRIBUTION : INFORMATION CAN ALSO BE DISTRIBUTED VIA THE ICT WEBSITE

The association is responsible for posters and documents distributed by its members. Posters and documents must be directly related to the purpose of the association and bear its acronym or logo. The right to display posters is strictly limited to the panels provided for this purpose or freely accessible. Any use of the lCT logo on paper or electronic media must be authorised in advance by the Vice-Rector for Student Life and Development.

and the Communications Department at the request of the BVE at least 15 days before the planned printing/distribution date. Any posting that does not respect the values and rules of the lCT will be automatically withdrawn by the administration.

USE OF CAMPUS DIGITAL RESOURCES (NETWORK/MESSAGING)

As regards the use of network resources in general and email in particular, associations are required to comply with the provisions of the lCT's IT charter. All recognised associations are allocated an e-mail address at the associationname@ict-toulouse.fr. This address is a mailing list for members of the association's executive committee. Subscribers are managed by the association itself. Any recognised association may, via the lCT's Student Life service, circulate electronic messages promoting projects supported by the university.

ALLOCATION OF FINANCIAL AID

Associations may receive annual financial assistance from the lCT for their operations. An application for financial aid must be completed and sent to the Student Life Office (BVE). Associations receiving financial aid must justify their use after the event by producing a moral and financial report on the action. This justification is a condition for the possible renewal of the aid.

SERVICES FOR LEARNERS

Students can take part in activities organised by Student Life, Community Involvement, Chaplaincy and Cultural Life. They have access to the SOIE. The Student Centre, shared work spaces, the Saint Dominique room and the ICT Café are all available to them (see the internal rules for these areas where applicable).