OMNES Education Group

Terms of Use for IT Resources/Equipment

1. PURPOSE

The purpose of the present Terms of Use for IT Resources/Equipment is to define the correct use of the resources made available by the School and to establish the responsibilities and obligations of each User; in particular with regard to protecting the Resources from any risk of damage, destruction and/or loss and to ensure data security and confidentiality.

The term « **School** » means the institution from which the student is studying for a period of time and will receive credits for these modules .

The term « **User** » means any student using, consulting or implementing Resources.

The term « **Resources** » refers to all IT Resources, communication tools and information made available to Users by OMNES Education London School (OELS). These resources and their contents may be the property of the OMNES Education Group.

The term « **Administrators** » refers to the people in charge of the effective operation and maintenance of the Resources, whether they are staff members, service providers and/or, where applicable, students under the responsibility of any of the former.

The term « **Education Managers** » refers to all faculty members, lecturers, and registrar's officers.

The User having read these 'Terms of Use' agrees to sign them, and to comply with them until the termination of their access to the Resources.

These Terms of Use are available on the internal interactive platform.

They are liable to be modified at any time, as a result of technical developments.

Users may be required to confirm that they agree to the Terms of Use several times during their schooling, or even, for alumni, after leaving the school.

2. DEFINITIONS

2.1. School Resources

Resources include Hardware and Software.

Hardware:

The resources concerned are fixed or mobile equipment and devices, including the personal material of the Users and/or third parties connected intermittently to the Resources (by

modem, by Internet, by a wireless network, by VPN or by any other means), such as servers, workstations, microcomputers, network infrastructures present on the School campuses, as well as all their peripherals (printers, mice, keyboards, ...).

Software:

All software resources, bespoke or standard, accessible from the School's networks both inside and outside the School premises.

2.2. Communication tools

Communication tools include all means of telecommunication: access to internal and external networks (internet), internet portals, internal interactive platform, electronic mail, video conferencing, instant messaging, schedule management…

2.3. Information

Information includes all the data, files, databases, images, sounds, texts and any exchange of information processed by the OMNES Education Group information system; as well as the student card made available to the User.

3. TERMS OF USE OF RESOURCES

Use of Resources is limited to educational activities (teaching, technical and software research and development, technology transfer, dissemination of scientific, technical and cultural information, trials of new technically innovative services); professional activities (internship research, finding a first position); the activities of associations; and incidental administrative and/or management tasks required by the above activities.

Users are required to log in to School Resources (such as Teams) with their own School IT Accounts.

For students who are not already registered with any of the schools owned by the OMNES Education Group, they are registered within the student database management system and network accounts are provided by OELS for the purpose of accessing the online platforms and for enhancing communications with the school administration and faculty.

Similarly, Users must use the Resources provided by the School (such as Teams, Boostcamp, ‘Hyperplanning’ scheduling software) required by the student-faculty interaction.

Any new resource must be approved in advance by the persons responsible for the proper functioning of the Resources, whether they are staff members, service providers and/or students under the responsibility of the former (the “Administrators”).

Any new activity is subject to the prior approval from the Administrators.

Lastly, the Resources shall only be used with the utmost respect for the lecturers, the staff of the School and the other students, which implies in particular not circulating any prohibited information (information that offends against human dignity, incites racial hatred or is of a pornographic nature etc.)

Recordings without a lecturer’s and other students’ consent are strictly prohibited.

4. TERMS OF ACCESS TO RESOURCES

The use of the Resources is subject to the approval of the School, before an individual User computer account with a unique username and a personal password is created (hereinafter "the IT Account").

The access rights granted are controllable, auditable and may be periodically revalidated by the School to comply with the security rules of the information system.

Opening an account:

The provisioning of your IT Account is confirmed with an e-mail sent from the Information Systems Department, and by acceptance of the Terms of Use by the User.

Access is strictly personal and non-transferable, even temporarily. A User who gives a third-party access is fully liable for any direct or indirect damages that may ensue (e.g. identity theft) under the conditions of the article covering "Liability" (see article 13).

Closure of an account:

Access to Resources may be withdrawn at any time, completely or partially, particularly if the User does not respect the Terms of Use.

The User's right of access to Resources is terminated in case of withdrawal from the course, dropping out of school and/or failing to graduate, non-payment of fees, and permanent exclusion from the school: the IT Account and its contents are then blocked and/or deleted.

Prior to their departure, the User will, if necessary, recover any personal data and information, and then delete them from the School's systems.

In case of non-payment of fees, access to Resources may be suspended until the fees are recovered by the school finance department.

5. SYSTEM LOG FILES

Users access to and use of the Resources may be recorded, for example in "temporary files" (or "logs") mainly for the purpose of verifying the operational standards of the computer systems.

The Administrators can also have access, to these logs as stipulated in the Terms of Use (see article 12 "Information Systems Administrators").

The Logs are stored for a duration of up to three years, in accordance with the legal provisions in force and the specifications of the CNIL (the French data protection authority), so that proof of any illegal acts can be provided.

6. STUDENT CARD AND PRINTING

A student card is provided free of charge when you first join the School. Should this card be lost, a replacement card must be purchased from the School's reception for the sum of £15. In case of theft, subject to the presentation of a police report, a new card is provided free of charge.

When the printing quota is reached, the User can update the printing account online via the Resources. Any quota remaining at the end of the school year or after graduation cannot be deferred or refunded.

7. ONLINE PROCEDURES

7.1. Online examinations

Users may be required to take their examinations remotely from their campus during their studies.

Online examinations may involve setting up an e-examination solution which remains under the control of the Administrators.

Participation in an examination via an E-exam solution may involve the student's consent to - installing a particular software on the student's computer. In the event that the student refuses to give consent, the student will be required to sit the examination in person in the School premises.

This e-examination solution provides means to faculty to create and schedule assessments and for students to be able to take the exam.

In order to perform this task students must enter their name, first name, email address and student number in the e-examination solution so that faculty can grade their work and provide the students with their results and comments.

The access codes given to the Users are strictly personal and confidential. In case of disclosure of codes or fraud, the disciplinary measures laid down in the Schools' regulations will be applied.

In order to limit cases of fraud, a system of remote monitoring of examinations shall be implemented. This monitoring system can use different technologies, in particular continuous video, random photography, remote monitoring with or without fraud detection algorithms, the use of a tool allowing a supervisor to remotely take control of the student's computer.

7.2. Paperless transcripts

The student's transcripts is converted to paperless and is under the control of the Administrators. The students may receive their transcripts directly by electronic communication means .

It is strictly forbidden to modify any document issued by the School (transcripts, diplomas, etc.) or to make fraudulent use of them.

7.3. Paperless attendance report sheet

Users may be required to sign an attendance sheet online using the IT resources provided by the School.

The signing of attendance sheets may involve the implementation of an online attendance solution which remains under the control of the Administrators.

Using the online signing process may involve the student's consent to installing software on their computer or mobile phone.

For this purpose, the following User data will be filled in on the online attendance solution: their surnames, their first names, their email addresses, the name of the course they are taking and their signatures.

7.4. Distance learning

Students may be required to take distance learning courses using the IT resources provided by the School during the course of their studies.

At the start of each distance learning course, students must switch on the video and audio systems of their computers so that the teachers can check the identity of each participating student.

7.5. Blended courses

In the context of blended courses, the speakers are filmed to enable remote students to follow the course.

In this context, students may be filmed on a temporary basis (e.g. during a face-to-face presentation).

8. INTERNET ACCESS REGULATIONS

As part of their access to Resources, students have access to an Internet connection.

Any breach of the rules on the use of the Internet (whether legal regulations, «customs and practices ", etc.), and, in particular, breaches of the rules mentioned below may give rise to sanctions under the conditions provided for in the article "Liability" (see Article 13).

8.1. Access to internal & external networks

Access to internal and external sites must be in accordance with the current rules on networks (including the Communications Regulations – Access to infrastructure - 2016).

It is expressly forbidden to:

- Use the Resources to engage in any action that may jeopardize the security or operation of the sites in question, (e.g. hacking).
- Connect or attempt to connect to a private site without the explicit authorization of its administrators (e.g. due to a problem, the private network (extranet) of a company becomes accessible to all, although it is possible to access this network, doing so is nonetheless an offense).

8.2. Protection of personal data

The diffusion of personal data by the User via the Resources must comply with the regulations in force and most notably The Data Protection act of 2018 (GDPR). The data voluntarily recorded by Users is their sole responsibility. It may be checked by the Administrators and possibly deleted if it is not in keeping with the purpose and ethics of the School.

8.3. Intellectual property

8.3.1 Resources

The User must not reproduce, download, copy, distribute, modify or use software, databases, web pages, images, photographs or other creations protected by copyright or exclusive rights, without the prior authorization of the holders of these rights.

It is prohibited to install, on the Resources, software or any other document, anything which is in violation of copyright and associated licenses.

The terms of redistribution of free software must be adhered to.

Thus:

- No copy of a file used within the School may be made unless the license associated with the file permits it. When in doubt, the User agree to consult the Administrators.
- It is forbidden to install and/or uninstall any software from the Resources, without the explicit agreement of the Administrators who must first check the validity of the license and the material requirements.

8.3.2 Courses

Faculty may deliver distance or in person courses.

Except if expressly authorized by the teacher, students are not allowed to record courses.

It is reminded that any reproduction, by any means whatsoever, or any distribution, in any medium whatsoever, of a distance or face-to-face course, without the express authorization of the lecturer concerned, is prohibited.

Users are reminded that they are not authorized to broadcast courses on social networks without prior authorization from the Faculty and may be subject to the disciplinary measures provided for in the School's internal regulations, notwithstanding any sanctions incurred in the event of failure to respect copyright and/or image rights.

8.4. Communication

The User cannot speak on behalf of the School or commit the School without having been duly authorized. They must show courtesy towards their interlocutors in electronic exchanges.

9. E-MAILS, DISCUSSION FORUMS AND SOCIAL NETWORKS

9.1. Rules for the use of e-mails

Each User is provided with their own personal School e-mail address and e-mail box.

Written communications between the School and the User, when made by e-mail, will primarily be sent to these e-mail addresses. The School cannot be held responsible if the User fails to read messages sent by a member of the School via this messaging system.

The size of the e-mail box made available to the student is limited. The User agrees to delete out- of-date/redundant e-mails to avoid saturation which could prevent the receipt of new e-mails.

9.2. Common rules governing use of e-mails, discussion forums and social networks

Any e-mail requires courtesy, respect and politeness. When an idea is not yours, give the author’s name.

Give precise, concise explanations.

Do not send large files except in forums clearly identified for this. Never send advertising (spam) messages via any medium.

It is vital to comply with these rules. Your image and that of the School on the Internet depend on it.

10. RULES OF USE AND SECURITY

10.1. Security

All Users are accountable for the use they make of the Resources made available to them by the School, they must therefore take responsibility for security.

It is prohibited to connect any devices to the Resources (computers, laptops, printers, modems, etc.) other than those provided for this purpose, except with the prior agreement of the Administrators.

Access to Resources including School networks, private networks, etc. by a "Wireless" connection (radio, infrared, etc.) is possible throughout the campus.

By default, access is prohibited during academic sessions (lectures, workshops, exams, etc.), without the express authorization of the person in charge of the session.

The same applies to the use of peripherals (personal computers, PDAs, etc.), even if not connected to the Resources.

In addition, all Users must protect their data, have a strong password and assure all due measures are taken to prevent any unauthorized person from accessing their private information.

User password must meet the following requirements:

- Be at least 8 characters long. These characters must include uppercase, lowercase letters, numbers, and punctuation.
- Be complex enough not to be found easily. Under no circumstances should it be a dictionary word, name, first name, pseudonym, phone number, credit card or license plate or any other another word that can be easily associated with the User.
- Not be used on another system outside the School.
- Not be communicated to anyone, UNDER ANY PRETEXT, even to the User's partner or the Administrators: if need be, administrators have the necessary rights to access any pertinent information.
- Be changed as soon as it becomes known to a third party.
- It is advisable to change the password regularly (the procedure for doing so is explained when the access is opened).

Finally, all User agree not to leave the equipment available to them unattended.

10.2. Usage

The User must not attempt to read and/or copy and/or disclose and/or modify and/or destroy the information of another User without their explicit authorization.

In particular, the User:

- Must not connect or try to connect to a server other than by the channel(s) provided for by this server or without the permission of authorized personnel.
- Must not engage in actions that knowingly endanger the security or normal operation of the servers they access.
- Must not assume the identity of another person.
- Must not intercept communications between third parties and must refrain from any interference in the transmission of messages to respect the confidentiality of private

correspondence. This rule also applies to private e-mail correspondence in which the User is not the addressee either directly or in copy.
- Must not use the Resources to offer or make available to third-parties, data and information that is confidential or contrary to the legislation in force.
- Must not register documents on a server unless the server allows this, or without the permission of authorized personnel.
- Must not attempt to expropriate an account to which access has not been authorized by the Administrators or attempt to decrypt the password of another User.
- Must show courtesy towards their interlocutors in electronic exchanges by mail, in discussion forums.
- Will not express personal opinions unrelated to the User's professional or academic activity, that may be detrimental to the OMNES Education Schools and Entities.
- Must obey the law, especially those relating to publications which are illegal, abusive, racist, pornographic, defamatory, xenophobic or paedophile; and must not violate privacy and image reproduction rights.

The School cannot be held responsible for the deterioration of information or offenses committed by a User who has not complied with these rules, and may, in case of legal action sue the User at fault, as stated in the conditions of the article "Liability".

10.3. Prohibited activities

In particular:

- Games, game emulators, pornographic activities, financial activities (trading, lottery, surfing in exchange for advertising, etc.).
- Programmes intended to impersonate a third party, to recover their username/ passwords, or test the security of a system.
- Writing and editing data on local computer disks, in directories other than temporary directories.
- The connection of wireless access points to the school wired network (pirate access points or WIFI card activated in a PC).

10.4. Respect for the individual

It is prohibited to hide one's true identity or to use a pseudo masking one's identity.

Programmes that may harm other users are prohibited: insults, harassment, bypassing security, resource saturation, viruses, unlocking software protection.

In general, terms, any action that could harm a person physically or morally is prohibited.

This includes diffusion of information of any kind (texts, images, sounds ...):

- Unverified or defamatory.

- Likely to infringe the privacy or image of others, or to damage the effective running of the School, its staff and its students.

10.5. Respect equipment made available to teachers and students for collective use

Each User must ensure that the equipment remains in good condition. Damaging or monopolizing equipment penalizes all Users.

Thus each User must:

- When working, use the device best adapted to the task.
- Not smoke, bring food or drink or leave mobile phones connected, in areas reserved for computer use.
- Not disconnect or use for other devices the cables set up by the IT department, whether they are connected to Resources or not.
- Not block a machine at peak times.
- When a device is being used for a non-educational use, the User must give way to a student wishing to work, if requested to do so.
- Lock workstations if absent for more than 5 minutes (especially during lunch hours).
- Never turn devices off: suddenly shutting down or restarting a device is prohibited. If the device crashes, contact the Administrators.
- Ensure, when leaving the device, that the equipment is in the condition that they would like to find it (material stored tidily, temporary and/or personal files deleted, session closed properly, ...).
- Regularly check/protect your USB flash drives and other devices against viruses. Avoid transferring executable files as much as possible. In general, do not execute the executable files found in emails.
- Limit the use of printers, especially during peak periods. For listings, use the "two pages per sheet" feature.
- Report any attempted infringement / intrusion, successful or not, to the Administrators (see Article 12).

As there are no quotas, Users must check that the disk space used by their data does not interfere with the work of other Users:

- The User must regularly check that the size of their personal accounts does not exceed that authorized by the Administrators;
- At the end of each school year, before going on vacation, each User must remove from their account data that has become redundant, especially at the end of their schooling;
- Any theft or deliberate damage of materials will be severely punished (see article 13). Anyone witnessing theft or damage must inform the site IT managers.

11. RULES FOR THE USE INTERNET SERVICES

Use of the Internet services as part of, or related to, school activities, must comply with the general principles and rules specific to the various sites accessed, and to the legislation in force.

Standard access to external networks (the Internet) must be made only from networks identified as user networks.

Access from these networks is nominative: Users must first log on their account to be able to access the Internet.

Access is nominative in order to prove any activity which is potentially illegal or contrary to the Terms of Use, and to preserve the security of the Resources.

Access to certain external sites is limited:

The list of blocked or low priority sites is defined by the Information Systems Department (it includes sites identified as containing malicious programs, child pornography sites, illegal download sites, etc.).

Filtering is based on URL lists established by specialized companies.

These lists of blocked sites may be incomplete or, on the contrary, include legitimate sites.

These errors should be brought to the attention of Administrators to have access restored or blocked as appropriate.

12. INFORMATION SYSTEMS ADMINISTRATORS

12.1. Compliance with the Terms of Use

The Administrators ensure the efficient running of the Resources and the compliance with the rights and duties of Users under these Terms of Use.

If there is infringement of the Terms of Use, the Administrators may refer the matter to the School Disciplinary Board, which will decide on any sanctions or measures to be taken.

12.2. Maintenance

To ensure the efficient running of the Resources, the Administrators reserve the right to suspend, for a specified period, the services and/or access to the Resources for maintenance. These interruptions will be minimized as much as possible.

Administrators may also reduce or remove (with or without notice) a User's access to the Resources, if this use becomes abusive and/or presents a security risk (machine time, disk space, bandwidth, software/files which are illegal or prohibited under these Terms of Use, viruses, etc.).

They may also generate and view event logs, and record User activity on Resources, if needed.

They may generate statistics to facilitate effective management of Resources: optimization, security, and misuse detection.

They may make backups of certain disks, including those hosting User data and email.

They may carry out any troubleshooting task on the Resources, as well as on any personal machine connected to the internal network. They may disconnect a suspect device, physically or from a distance.

12.3. Right to investigate and confidentiality obligation

The Administrators are subject, in the execution of their role, to a duty of confidentiality. To ensure the efficient running and security of the Resources, they may carry out the necessary investigations and access Users' private data (e-mails, processes, files, work sessions, logs, etc.).

In the framework of their duty of confidentiality, among other things, they are not allowed to divulge the information learned by research into Users' private data.

However, when a search is made necessary by the discovery of criminal acts, they may explore the Users' data and provide excerpts to the school management and/or to the appropriate police department.

12.4. Administrators Responsibility

The School/Administrators are in no way responsible for personal equipment; the Users is solely responsible for the security and protection of these devices. The School/ Administrators cannot be held liable for direct and/or indirect damages suffered by the Users when using the Resources within the School.

13. LIABILITY AND SANCTIONS INCURRED FOR NON- COMPLIANCE WITH THESE TERMS OF USE

Infringement of the rules as defined in these Terms of Use may incur the civil liability of the User and lead to disciplinary action such as:

- Termination of access to the Resource (s).
- Appearance before the Disciplinary Committee. The latter can rule on the exclusion of the User and result in legal proceedings.

In addition, each User must ensure, to avoid civil and/or criminal liability, that the content of their communications does not infringe the legislation in force, in particular relating to:

- Protection of personal data.
- Protection of intellectual property rights, including software.

- Computer fraud.
- The content of information diffused by a User.

In general, the laws can be reviewed online on the official government website at:

https://www.legislation.gov.uk/

Everyone must ensure they respect the texts mentioned above and those of these Terms of Use.

14. INFORMATION TECHNOLOGY AND LIBERTY

14.1. Processing personal data

The personal data of Users processed by the School is for the exclusive use of the School and its students and will under no circumstances be shared externally, other than those circumstances communicated to the Users, such as for the Extranet system allowing links with companies for the purpose of internship research, " student jobs" or employment, or the publication of data on the School site.

14.2. Video surveillance

For the safety of Users, all School premises, including the annexes to the main building, are placed under video surveillance. An Administrator can record, view and export sections of the recorded stream for the purpose of investigation of any crime or offence committed on the school premises. The record data is overwritten after a period of 3 months maximum.

15. VALIDATION OF THE TERMS OF USE

The current Terms of Use are valid as long as the User's account is open. It may need to be updated each year.

The User declares that he/she has read these Terms of Use and the related laws and undertakes to respect them:

- By an electronic signature **OR;**
- By ticking the box on the school's registration site.