



28 January 2022

MEMORANDUM

Ref.: 2022-01-M-2-en-1

Orig.: EN

To : OSG's and European Schools' staff members

From : Andreas Beckmann, Secretary-General

Subject : Charter for the use of ICT Resources by the European Schools' and the OSG's staff members¹

Dear colleagues,

The Charter for the use of ICT Resources by the European Schools' and the OSG's staff members from 2011² and its Protocol on the access to the Staff members' emails and documents in case of absence³ have been updated. In consequence, this updated version cancels and replaces all previous documents in that regard.

The Charter aims to provide interpretation of the duty of confidentiality set forth in Article 10 of the Service Regulations for the Administrative and Ancillary Staff, Articles 18 of the Service Regulations for the Seconded Staff, Article 19 of the Service Regulations for the Locally Recruited Managerial Staff and Article 25 of the Service Regulation for the Locally Recruited Teachers. In accordance with the Service Regulations applicable to them, staff members should be requested to sign the Confidentiality Agreement provided in Annex II of the Charter.

¹ 2021-10-D-72-en-1.

² Memorandum 2011-11-M-2.

³ Annex I of the Charter.


The Charter also sets out the rules for proper use and good behavior vis-à-vis the use of the ICT resources provided by the IT technicians and the ICT Unit to the staff members⁴ and any guest⁵ of the European Schools or the Office of the Secretary-General.

In this sense, the Charter should be notified to all the staff members and be published on the Schools' and the OSG's website.

Please note that Annex III and IV provide guidelines for the staff members' departure procedure and for the use of social media by teachers, respectively. These guidelines are intended to inspire the Schools and the OSG to adopt their own departure procedure and social media policy.

The Directors are requested to support the compliance with the Charter and its annexes.

This MEMORANDUM will be subject to a review by January 2024.



Andreas BECKMANN
Secretary-General

ANNEX:

- Charter for the use of ICT resources by the European Schools' and the OSG's staff members (2021-10-D-72-en-1)
 - **Annex I:** Protocol on the access to the Staff members' emails and documents in case of absence (2021-10-D-71-en-1),
 - **Annex II:** Confidentiality agreement (2021-10-D-73-en-1),
 - **Annex III:** Guidelines for the staff members' departure procedure (2021-10-D-74-en-1),
 - **Annex IV:** Guidelines for the use of social media by teachers (2021-12-D-09-en-1).

⁴ Administrative and Ancillary Staff ('AAS'), Seconded staff, Locally Recruited Managerial Staff, temporary staff members (trainees, interim).

⁵ Any person who is invited by the OSG/European School to participate to a meeting, a working group or a training and who is provided with access to ICT resources or has a European Schools' account.



Schola Europaea

Scuola Europea di Varese

Ref.: 2021-10-D-72-en-1

Orig.: EN

CHARTER FOR THE USE OF ICT RESOURCES BY THE EUROPEAN SCHOOLS' AND THE OSG'S STAFF MEMBERS

Annex to MEMO 2022-01-M-2

Contents

CHARTER FOR THE USE OF ICT RESOURCES	4
PREAMBLE	4
1. SCOPE.....	4
2. DEFINITIONS.....	4
3. ACCEPTABLE USE AND OWNERSHIP	5
4. GENERAL RULES OF GOOD BEHAVIOR.....	5
4.1 Duty of care.....	5
4.2 Duty of confidentiality	5
5. SPECIFIC RULES	6
5.1 Files and documents	6
5.2 Network and internet use	6
5.3 Accounts and passwords	7
5.4 Electronic communications.....	7
5.5 Teaching	9
6. PERSONAL DATA BREACH.....	9
7. MONITORING	10
8. SANCTIONS	10
9. NATIONAL LAW	11
10. CHANGES.....	11
ANNEX I	12
1. PRINCIPLES OF FINALITY AND PROPORTIONALITY.....	14
2. CONTROLLER'S APPROVAL.....	14
3. RIGHT TO BE INFORMED.....	14
4. LIMITED ACCESS.....	15
4.1 Limited scope	15
4.2 Limited time.....	15
4.3 Limited authorised persons	15
5. RETENTION PERIODS.....	16
ANNEX II	19
ANNEX III	22
1. RESPONSIBILITY	24
2. WORK HANDOVER PROCESS.....	24
3. HANDOVER OF EQUIPMENT	24
4. PERMISSIONS AND ACCESSES.....	25
ANNEX IV	26

PRELIMINARY REMARKS.....	27
1. DEFINITION OF THE PEDAGOGICAL PURPOSES.....	27
2. ACCOUNT CREATION	27
3. SOCIAL MEDIA CHARTER	28



Schola Europaea

Scuola Europea di Varese

Charter for the use of ICT resources by the European Schools' staff members

PREAMBLE

This Charter sets out the rules for proper use and good behavior vis-à-vis the use of the ICT resources provided by the IT technicians to the staff members¹ and any guest² of the European School (hereinafter referred to as the "School").

Having such Charter in place helps to protect both the OSG and the Schools as well as the staff members. Inappropriate use of ICT resources exposes to risks including virus attacks, compromise of network systems and services, as well as legal issues.

This Charter cancels and replaces all previous documents in that regard.

1. SCOPE

Such Charter is provided to the School's management and staff members (hereinafter referred to as the "staff members") during the onboarding process or subsequently when an updated version is available, and to any guest being provided with the School's ICT resources.

Such Charter forms an annex to the House Rules of the School and falls within the framework of the laws and regulations in force relating in particular to copyright, intellectual property rights, privacy protection (including in particular image rights) and to the processing of personal data, as well as computer crime.

2. DEFINITIONS

"ICT resources" means generally all hardware devices (laptops, workstations, mobile phones, periphery devices, interactive whiteboards, etc.), networking services, as well as all software resources (applications, databases) locally or remotely accessible made available and administrated by the ES.

"ICT Unit" means the OSG's ICT Unit and its staff members.

¹ Administrative and Ancillary Staff ('AAS'), Seconded staff, Locally Recruited Managerial Staff, temporary staff members (trainees, interim).

² Any person who is invited to the OSG/School to participate to a meeting, a working group or a training and who is provided with access to ICT resources or has a European Schools' account.

“IT technicians” means the local ICT staff members of the schools.

“Networking services” means the provision to local and remote services such as applications, messaging, web, conferencing etc. through the networking infrastructure of the ES.

“User” means the person having access to or using ICT resources and networking services no matter what his/her status may be.

3. ACCEPTABLE USE AND OWNERSHIP

The School’s ICT resources are intended to be used for the achievement of the staff members’ professional tasks, pursuant to their contractual or statutory relationship with the School.

Use of the ICT resources for personal purposes is not prohibited but staff members are expected to exercise good judgement and remain productive at work while using them for personal-related matters.

Staff members should be aware that the professional files and documents created through the School’s ICT resources that fall within the scope of their employment or secondment as well as the tasks assigned to them become the property of the School.

For cyber security and maintenance purposes, the ICT resources of the School such as equipment, systems and network traffic can be monitored at any time.

All documents, licenses, software provided through the ICT resources are the property of the School and must not be copied, altered, modified or transferred without a prior authorization.

4. GENERAL RULES OF GOOD BEHAVIOR

4.1 Duty of care

Staff members are expected to exercise care in the use of the School’s ICT resources. Loss, damage or theft of the School’s property should be reported at once to the School’s IT technicians.

Negligence in the care and use of School’s property may be considered grounds for disciplinary sanctions.

4.2 Duty of confidentiality

All staff members are bound by a legal duty of confidentiality³ to protect the personal information they have access to in the course or in connection with the performance of their duties. They are requested to sign the confidentiality agreement (Annex II) during the onboarding process or subsequently when an updated version is available.

³ See the Services Regulations of the European Schools’ staff members:

- Article 18 of the Service Regulations for the Seconded Staff,
- Article 19 of the Service Regulations for the Locally Recruited Managerial Staff,
- Article 10 of the Service Regulations for the Administrative and Ancillary Staff,
- Article 25 of the Service Regulation for the Locally Recruited Teachers.

More particularly, this duty of confidentiality applies to all information made available through the ICT resources provided to the staff members.

In the event staff members have access to resources that it would be inappropriate for them to have, they have the responsibility to notify the ICT Unit/IT technicians so the problem can be corrected.

5. SPECIFIC RULES

5.1 Files and documents

5.1.1 Storage

Staff members must save their professional files and documents in their device's personal storage space and/or in a shared storage space if other colleagues and/or their Head of Unit also need to consult them.

As stated above, ICT resources are intended to be used for professional purposes, but private documents could be stored on the staff member's device **as long as they do not contain other persons' personal data**. Such documents must be kept in a folder called "PRIVATE".

Staff members must be aware that in the event of a data breach, their private documents may be impacted.

5.1.2 Clean desk policy

Staff members must be aware that leaving documents on their desk may lead to unauthorized access. No documents containing confidential information should be left out on desks, or in the printer.

5.1.3 Prohibition

In particular, files and/or documents contrary to public order and morality or illegal, such as -for example- racist, xenophobic or pornographic content are strictly forbidden.

5.2 Network and internet use

Users are responsible for the appropriate use of the network resources and internet.

Use of a private digital device does not exempt users from following the rules laid down in this Charter, as regards respect for their colleagues and the members of the European Schools' community.

Furthermore, the use of social media -through ICT resources or a private digital device- does not exempt the users from being responsible for the content they disclose.

Users should:

- Log into their professional account only from secure devices and avoid the use of public free Wi-Fi,
- Lock their devices when leaving them unattended,

- Use extreme caution when opening email attachments received from unknown senders,
- Report to the School's IT technicians any suspicious electronic communication,
- Exercise good judgment regarding the reasonableness of personal use.

Users are prohibited from:

- Accessing a server, personal data or an account for any purpose other than carrying out your professional tasks, even if you have authorized access,
- Sending confidential information to unauthorized recipients,
- Connecting to social media with the email address linked to their professional account,
- Posting or publishing content on social media that is neither inappropriate nor harmful to their colleagues and the members of the European Schools' community,
- Accessing, downloading or uploading obscene, offensive, discriminatory or other material prohibited by the law,
- Unlawful downloading or uploading of any copyrighted material (i.e.; pictures, music, video and software),
- Downloading, installing or running any upgrades, updates, patches or any program, software whatsoever,
- Researching and altering the security of the ICT solutions provided without prior authorization,
- Making use of any security holes or anomalies in system operations.

5.3 Accounts and passwords

Accounts are created (manually or automatically) by the staff of the ICT Unit. They are temporary, strictly personal and non-transferable. They shall be deactivated when the holder leaves the organization.

User should:

- Set their password in accordance with the instructions provided by the ICT Unit,
- Use strong password and keep them confidential,
- Immediately inform the system administrators if the misuse of the personal account is detected or suspected.

Users are prohibited from sharing and revealing their account and password to third persons (including system administrators) or allowing the use of their account by others.

5.4 Electronic communications

5.4.1 General considerations

Staff members and users are responsible for managing their email, chat and any other communications content while using the School's ICT resources.

They are prohibited from:

- Using the lists of email addresses or any other communication channels for purposes other than those intended by professional objectives,
- Using improper language in their communications,
- Sending unsolicited (commercial or otherwise), unwanted or harassing communications.

As electronic communications are intended to be used for the achievement of the staff members' professional tasks, the use of such communications for personal-related matters should be limited. In such case, staff members should label their electronic communication as "PRIVATE".

Functional and shared mailboxes must never be used to send electronic communications that are not related to the staff member's professional tasks.

5.4.2 Absence of a staff member

In the event staff members are unable to access their electronic communications, they are expected to have the necessary arrangements in place to ensure continuity of the School's activities, by:

- Activating an "out of office" automatic reply in Outlook and indicating a colleague's contact information as well as a status message in Teams whereby colleagues are informed of the absence,
- Using shared folders where the information is accessible to the back-up colleagues and/or to anyone with a functional interest in accessing it during the absence.

Forwarding emails during the staff member's absence is not advisable as the new recipient might become aware of potentially sensitive information without the knowledge of either the sender or the absent staff member.

In exceptional circumstances and if no arrangements could be foreseen prior to the staff member's absence, the School may allow the access to the personal mailbox in accordance with the conditions set forth in Annex I. Such access must comply with:

- The principle of finality,
- The principle of proportionality,
- The principle of transparency.

Due to data protection requirements⁴, the access to staff members' mailboxes and documents who have definitely left the European

⁴ Principles of purpose limitation, data minimisation and storage limitation.

Schools system (i.e.; dismissal or departure) is not possible. All work-related material and documents should be handed over according to the instructions given by the staff members' superiors before their departure (see Annex III).

5.5 Teaching

5.5.1 Distance Teaching and Learning

Teachers must follow the provisions of the Distance Teaching and Learning Policy for the European Schools as approved by the Board of Governors on 29 March 2021⁵.

5.5.2 Digital Learning Resources

Teachers who need to use digital resources that are designed and intended to be used for educational and/or pedagogical purposes must consult their School's DPO.

The latter will assess such resources pursuant to the Procedure for the use of a Digital Learning Resource within the European Schools⁶.

5.5.3 Social media

A distinction is essential regarding the use of social media:

- Social media are not covered by the above-mentioned procedure as the teachers must not use pupils' personal data on social media platforms,
- Teachers must not encourage pupils to create individual accounts on social media,
- Teachers are allowed to create an account on social media for educational and/or pedagogical purposes pursuant to the conditions set forth in Annex IV.

As explained in paragraph 5.2, teachers must not create an account on social media with their professional email address for security reasons.

6. PERSONAL DATA BREACH

Pursuant to the GDPR⁷, a personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

⁵ 2020-09-D-10.

⁶ 2020-01-D-9 Annex to MEMO 2019-12-M-3/GM. Such procedure relies on "legitimate interests pursued by the controller" as a legal basis.

⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ('General Data Protection Regulation').

Pursuant to the European Schools' Data Breach Policy⁸ staff members are encouraged to act promptly and report data breaches to the Director and/or to the DPO. They must also contact the IT technicians to immediately take the necessary actions in order to prevent and/or mitigate any negative consequences.

7. MONITORING

For cyber security reasons as well as for securing IT operations and maintenance, IT resources and network traffic can be monitored, analyzed and tested for compliance with and within the limits of applicable laws on a permanent or punctual basis, for:

- Prevention of cyber security incidents and attacks,
- Prevention of wrongful or defamatory acts, acts conflicting with morality or likely to impair other persons' dignity,
- Protection of economic or financial interests of the schools marked as confidential and the fight against contrary practices,
- Safety and/or the correct technical functioning of computer systems in the schools' network, including control of related costs, as well as the physical protection of school installations,
- Compliance in good faith with the principles and rules for using network technologies established in the European Schools system.

Such monitoring is mostly carried out by the ICT Unit -specifically for the administrative network-, while the School's IT are responsible for the pedagogical network.

Monitoring should be performed by automatic means whenever this is possible. Any manual intervention must observe the principle of proportionality and the system administrator must inform the staff member whose information is being monitored about the details of the intervention.

If the purpose of the manual intervention is to ensure compliance in good faith with the principles and rules for using network technologies established in the European Schools system, the intervention must be preceded by a prior information phase.

8. SANCTIONS

Any violation of the provisions of this Charter may be subject to disciplinary measures in accordance with the relevant Service Regulations:

- Title VI of the Regulations for Members of the Seconded Staff,
- Chapter VIII of the Service Regulations for the Administrative and Ancillary Staff,
- Chapter VIII of the Service Regulations for the Locally Recruited Teachers.

⁸ 2020-05-D-7 Annex to MEMO 2020-05-M-3-en-1/GM.

9. NATIONAL LAW

The provisions of this Charter shall not prejudice the application of more restrictive provisions from national law of the host country where the School is located.

10. CHANGES

This Charter may be subject to a review by January 2024.

ANNEX I



Schola Europaea

Scuola Europea di Varese

Ref.: 2021-10-D-71-en-1

Orig.: EN

Protocol on the access to the Staff members' emails and documents in case of absence

Annex to Charter for the use of ICT resources by the European Schools' and the OSG's staff members (2021-10-D-72)

Protocol on the access to the Staff members' emails and documents in case of absence

Contents

- 1. PRINCIPLES OF FINALITY AND PROPORTIONALITY 14
- 2. CONTROLLER'S APPROVAL..... 14
- 3. RIGHT TO BE INFORMED..... 14
- 4. LIMITED ACCESS..... 15
 - 4.1 Limited scope 15
 - 4.2 Limited time..... 15
 - 4.3 Limited authorised persons 15
- 5. RETENTION PERIODS..... 16

Protocol on the access to the Staff members' emails and documents in case of absence

The purpose of preventive measures as those indicated in paragraph 4.4.2 is to reduce the need to access to the staff members' mailbox and documents in case of an absence.

Where these preventive measures do not circumvent the employer's need to access an absent employee's emails and/or documents or where such measures were not taken by the employee before the absence, the present protocol determines how such access must be carried out to comply with legal and data protection considerations.

1. PRINCIPLES OF FINALITY AND PROPORTIONALITY

The purpose of ensuring continuity of service within the School constitutes a legitimate purpose to access the staff members' mailbox and documents as long as (i) there is a sense of urgency and (ii) there is no other less intrusive way to access to the needed information.

2. CONTROLLER'S APPROVAL

The need to access has to be duly justified in written using the form below.

Such form must be sent to the Director who will decide whether to authorize such access given the circumstances and considering whether:

- The information needed may be accessed in a less intrusive way,
- Such access is necessary for the continuity of the service,
- Such access is urgent or may be delayed given the length of the employee's absence,
- Such access should be authorized under additional precautionary measures that those set forth in the present annex.

The Director will also seek advice from the Data Protection Officer.

3. RIGHT TO BE INFORMED

Staff members are provided with the ICT Charter during the onboarding process or subsequently when an updated version is available. In consequence, they are informed about the possibility to access their mailbox and/or documents under the conditions set forth in the present protocol.

In the event the School does need to access a staff members' mailbox and/or documents, they have to be contacted by phone and provided with "*a detailed*

explanation for this access, outlining necessity, urgency, the nature and scope of the information sought⁹.

Besides the information to be provided under Article 13 of the GDPR¹⁰, staff members also have to be informed about their right to object under Article 21 of the GDPR.

When the staff member cannot be reached and the situation in question requires an urgent access, the Director may authorize the access in line with the present protocol.

4. LIMITED ACCESS

4.1 Limited scope

When authorization has been provided to ensure continuity of service, the access has to be limited to the emails and/or documents related to the period of the staff member's absence, or to a reasonable period prior to that absence.

The Director may authorize a more extended access if the reasons were clearly explained in the request submitted to him/her and are sufficiently justified.

Furthermore, only the emails and/or documents related to the request initially submitted for approval have to be consulted.

The emails and documents labelled as "PRIVATE" as indicated in the present Charter shall not be accessed.

4.2 Limited time

Once approval was granted, the access to the absent staff members' information must be limited to two working days.

4.3 Limited authorized persons

The Director designates the persons who have a legitimate interest in accessing the staff member's mailbox and/or documents.

The Schools' IT technicians need to request access rights from the ICT Unit as they do not have such accesses for the administrative network.

The access to the needed information must be carried out in the presence of another staff member (i.e.; staff representative, line manager, person in charge of HR, Head of Unit) and if possible, under the supervision of the ICT staff.

⁹Guidelines on personal data and electronic communications in the EU institutions, European Data Protection Board, February 2020.

¹⁰ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ('General Data Protection Regulation').

ICT staff will have to ensure that all necessary measures were taken, if needed, to ensure the security of the staff member's information (i.e., changing passwords).

5. RETENTION PERIODS

The DPO must be consulted regarding the storage of the information that was retrieved on the occasion of the access.



Schola Europaea

Scuola Europea di Varese

Form to be used to request access to an absent staff members' emails and/or documents in case of emergency

<p>Name of absent staff member <i>(whose information needs to be accessed)</i></p>	
<p>Name of the person requesting access</p>	
<p>Reasons of the access request <i>(Why is there a sense of urgency, why is this the only way to access the needed information, etc)</i></p>	
<p>Type of information needed</p>	
<p>Conclusion of the Director</p>	<p><input type="checkbox"/> Access granted <input type="checkbox"/> Access denied Date and time: Signature:</p>
<p>Staff member was informed by phone</p>	<p><input type="checkbox"/> Yes ... date/time <input type="checkbox"/> The person was not reachable</p>
<p>Name of the staff member(s) to be present during the access</p>	

To be filled in **during** access:

Actual date of access	Date and time ...
Name of the persons present during the access	
Observations <i>(Type of information to be consulted and timeframe)</i>	

To be filled in at **the end** of the access:

End of access	Date and time ...
Observations <i>(Type and timeframe of the information consulted, results of the consultation (information sought was whether found or not))</i>	
Name and signature of the person who had access	

ANNEX II



Schola Europaea

Scuola Europea di Varese

Ref.: 2021-10-D-73-en-1

Orig.: EN

Confidentiality agreement

Annex to Charter for the use of ICT resources by the European Schools' and the OSG's staff members (2021-10-D-72)



Schola Europaea

Scuola Europea di Varese

Confidentiality agreement

In accordance with the Staff Regulations applicable to them, all staff members are required to exercise the utmost discretion with regard to facts and information that come to their knowledge in the course of or in connection with the performance of their duties.

I, the undersigned, Mr./Ms. _____, working as _____ at the European School _____ (hereinafter referred to as the "School"), having access to confidential information and personal data belonging to the School, declare that I recognize the confidentiality of the said data.

I therefore undertake, in accordance with the requirements of the Staff Regulation applicable to me and the GDPR¹¹, to take all necessary precautions within the scope of my duties to protect the confidentiality of the information to which I have access, and in particular to prevent it from being altered, damaged or communicated to persons not expressly authorized to receive such information.

In particular, I undertake:

- not to use the data to which I may have access for purposes other than those provided for in my duties;
- not to divulge such data to any person other than those duly authorized, by virtue of their duties, to receive such data;
- not to make any copy of these data except as necessary for the performance of my duties;
- to take all necessary precautions to preserve the physical security of this data;

¹¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ('General Data Protection Regulation').

- to ensure, within the limits of my authority, that only secure means of communication are used to transfer such data and to consult the DPO in case of doubt;
- in the event of termination of my duties, to return all data, documents and any information support relating to these data.

This confidentiality agreement, which is in effect for the duration of my employment, will remain in effect without limitation of time after my termination of employment, regardless of the cause, insofar as this agreement relates to the use and disclosure of personal data or confidential information.

I have been informed that any violation of this commitment will expose me to disciplinary and criminal actions and sanctions in accordance with the legal provisions in force.

(City) _____, on _____ in _____ copies.

Name:

Signature:

ANNEX III



Schola Europaea

Scuola Europea di Varese

Ref.: 2021-10-D-74-en-1

Orig.: EN

Guidelines for the staff members' departure procedure

Annex to Charter for the use of ICT resources by the European Schools' and the OSG's staff members (2021-10-D-72)

GUIDELINES FOR THE STAFF MEMBERS' DEPARTURE PROCEDURE

Contents

1. RESPONSIBILITY	24
2. WORK HANDOVER PROCESS	24
3. HANDOVER OF EQUIPMENT	24
4. PERMISSIONS AND ACCESSES	25

GUIDELINES FOR THE STAFF MEMBERS' DEPARTURE PROCEDURE

The OSG and the European Schools must foresee a procedure that defines the process to be followed when a staff member is transferred to another school or definitely leaves the School.

The purpose of such procedure is to ensure minimal disruption of the work activities and the efficient transfer of all information contents, in compliance with data protection requirements.

Such procedure must cover at least the following items:

1. RESPONSIBILITY

The handover procedure is to be implemented primarily by the departing staff member. The person in charge of HR in the School is responsible for initiating and monitoring the handover process and ensuring that it is carried out in the School's best interest for the continuity of its activities.

2. WORK HANDOVER PROCESS

- Definition of a plan and timeframe for the handover of the School's information (i.e.; folders, files, documents, ...),
- Transfer of duties and knowledge to the departing staff member's replacement (i.e.; day-to-day activities, ongoing issues, access to relevant information, ...),
- Transfer of information in both electronic and paper form (i.e.; checklist of files, documents, archives, copy of relevant emails, ...) to the designated location and to the person in charge of HR in the School.

Such information should be stored on a shared information storage (i.e.; servers, filing cabinets, ...) used by the Unit, department and/or colleagues.

3. HANDOVER OF EQUIPMENT

The person in charge of HR in the School is responsible for:

- Compiling a list of all equipment and items to be retrieved/handed over and foresee who is charge of retrieving the School's professional equipment(s), badges, keys as well as professional mobiles, if any.
- Planning and informing the departing staff member about the terms of the handover to the designated person(s) and the defined timeframe.

4. PERMISSIONS AND ACCESSES

- Prior to his/her departure, the staff member in question must be allowed:
 - i. To collect his/her personal belongings,
 - ii. To collect or delete his/her private electronic communications,
 - iii. To destroy the documents that are no longer needed to ensure the continuity of the School's activities.
- The staff member must be informed about the deactivation of his/her account and the revocation of all his/her access rights to the School's resources at the day of the end of her/his contract. The content of the departing staff members' account will be deleted after the retention period of thirty days has expired, without prejudice to the rights set forth in Chapter III of the GDPR.
- The ICT Unit/IT and the ServiceDesk must be properly informed by the person in charge of HR in the School through a service request to the ES-ICT-SERVICEDESK@eursc.eu to require the deactivation of all accounts belonging to the departing staff member and the deletion of all content of these accounts after one calendar month.

ANNEX IV



Schola Europaea

Scuola Europea di Varese

Ref.: 2021-12-D-09-en-1

Orig.: EN

Guidelines for the use of social media by teachers

Annex to Charter for the use of ICT resources by the European Schools' and the OSG's staff members (2021-10-D-72)

GUIDELINES FOR THE USE OF SOCIAL MEDIA BY TEACHERS

These guidelines are intended to help teachers use social media in class with their pupils in a responsible, secure and reliable way, without harming the school's reputation or its community.

PRELIMINARY REMARKS

To ensure compliance with the GDPR requirements and applicable national laws, the European Schools do not allow pupils to create individual accounts on social media, as set forth in the ICT Charter for pupils.

Such platforms do not offer any guarantee in terms of privacy as their conditions of use cannot be negotiated by the Director of the School.

However, the School may allow the creation of an account on behalf of the class under the conditions set forth below.

1. DEFINITION OF THE PEDAGOGICAL PURPOSES

The teacher must guide the pupils towards a secure and responsible use. The pursued pedagogical purposes that are sought by the teacher when creating an account on social media for the class must be defined beforehand.

Such objectives may include:

- Acquisition of digital skills,
- Raising awareness about the Internet (*legal aspects, image rights, responsible attitude, e-reputation, awareness of the dangers*);
- Providing education in written and audiovisual media;
- Developing critical thinking skills;
- ...

2. ACCOUNT CREATION

The teacher is the one who creates the account and the password must not be shared with the pupils.

The account has to be created with a "temporary/disposable" email address, used for a short period of time, that can be discarded once it is no longer useful.

In other words, the "temporary/disposable" email address is an email address that is specifically created for the creation of the account on social media.

Such email address is needed to avoid security threats that could compromise the teachers' information as well as the School's.

3. SOCIAL MEDIA CHARTER

The teacher must draft a Charter for the use of social media together with the pupils in order to define the objectives of the project and raise awareness about the internet use.