COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Policy on the use of the Information System of the Council of Europe

1. Purpose of the Policy on the use of the Information System

1.1. The Council of Europe's patrimony of information constitutes one of its most important assets.

1.2. It includes intellectual capital – all the information derived from its activities and constituting its knowledge and expertise – the degradation or disclosure of which could harm its image; as well as information on its staff, the disclosure of which could constitute a violation of privacy or a breach of confidentiality.

1.3. The protection of this patrimony must take into account a complex organisational and technical environment characterised by the Organisation's broad functional and geographical scope, its use of a variety of technologies, a wide range of user profiles and its institutional relations with member States.

1.4. In this context, users of the Council of Europe's Information System have a key role to play in building and conserving this patrimony. They must ensure that they use the information technology (IT) resources and technological solutions provided by the Organisation in a sensible and responsible manner.

1.5. The purpose of this Policy is to set out the conditions governing access to and use of the Council of Europe's Information System; specify the rights and responsibilities of System users and of IT administrators using and managing the Information System; and regulate the relevant measures of supervision.

1.6. The rules governing the use of the Information System, as laid down in this Policy and specified in the IT administrators' charters and the Information System policies drawn up by the Directorate of Information Technology (hereinafter "DIT"), are intended to ensure the security and performance of the Council of Europe's Information System and preserve the confidentiality of data, in accordance with the applicable legislation and with the rights and freedoms of users.

2. Definitions

For the purposes of this Policy:

"**Information system**" means the Council of Europe's IT and telecommunication systems, i.e. tangible and intangible IT resources, comprising:

- Digital data, such as databases, files and electronic archives.
- Cloud computing solutions and network hard drives, i.e. storage spaces accessible only via a local network or the internet, used to store and process Council of Europe data.
- Hardware, meaning all of the Information System's tangible hardware components, such as desktop computers, telephone sets, portable devices, storage devices and other elements of the Information System's infrastructure.
- Software, i.e. all programmes, applications, operating systems, utilities, development tools and code used within the Information System to perform specific tasks.
- Documentation, such as system documentation, configuration documentation, user manuals and training materials.

"**Users**" means any person, whether a Secretariat member or a third party, who is subject to this Policy in accordance with paragraph 3.1 and who interacts with the Council of Europe's Information System. The term "users" includes IT administrators unless otherwise stated or specifically regulated.

"**IT administrators**" means any person who has privileged rights over all or part of the Information System, for operation, development, installation or any other purpose.

"Secretariat members" means permanent, local and temporary staff of the Council of Europe, seconded officials, trainees and study visitors.

Depending on the situation of the user concerned, the term "**relevant IT department**' refers to the Directorate of Information Technology of the Council of Europe or its IT Partners, namely the IT Departments of the European Court of Human Rights, the European Directorate for the Quality of Medicines and Health Care, the Parliamentary Assembly and the European Audiovisual Observatory.

The term **"Information System security**" refers to the ability of the Information System to withstand, with a given level of confidence, any action that could compromise the availability, authenticity, integrity or confidentiality of data being stored, transmitted or processed, or of the services it provides or to which it gives access.

"**Access rights"** means the extent to which a user has been granted access to specific parts of the Council of Europe's Information System, under the authority of the Secretary General.

"**Means of authentication**" means any form of identification such as username, password, security key, security token, PIN code, biometric traits, which is used to authenticate the user (in other words, to prove their identity) and to verify the extent of their access rights to the Information System.

In accordance with the Council of Europe Regulations on the Protection of Personal Data, [1] "**personal data**" means any information relating to an identified or identifiable individual.

"**Electronic communications**" means the transmission and reception of information by users through the Information System.

In accordance with the *Council of Europe Policy on the use of social media by Secretariat members*, the term "**social media**" refers to digital applications that enable users to create, share and interact with content publicly or within private groups, or to participate in social networking.

"**Security incident or breach**" means any weakness in the Information System that would enable a potentially malicious individual to interfere with its normal functioning or to gain access to data which they are not authorised to access, or any event that has an actual or potential negative impact on the security of the Information System by compromising the availability, authenticity, integrity or confidentiality of the data being stored, transmitted or processed or of the services that the Information System provides or to which it gives access.

"**Wrongdoing**" is defined in *Speak Up: Council of Europe Policy on reporting wrongdoing and protection from retaliation* (hereinafter referred to as the "Speak Up Policy").

[1] Resolution CM/Res(2022)14 establishing the Council of Europe Regulations on the Protection of Personal Data, adopted by the Committee of Ministers on 15 June 2022 at the 1437th meeting of the Ministers' Deputies.

3. Scope

3.1. The rules set out in this Policy apply to Secretariat members and to any other person – including, but not limited to, those working for external service providers – to whom access to the Council of Europe's Information System has been granted.

3.2. This Policy applies to all the activities of the Organisation, in any place where Secretariat members or other users have access to the Council of Europe's Information System and regardless of the means used to connect to it, including personal devices.

3.3. In cases of absolute necessity or emergency, derogations from the rules set out in this Policy are subject to explicit prior approval by the Secretary General and are granted only to the extent strictly necessary. DIT must be informed of such exceptions and oversees their implementation.

3.4. DIT is responsible for implementing this Policy. It shall produce and keep up-to-date more detailed texts regarding use and security which supplement this Policy and clarify its contents.

3.5. DIT, in liaison with the Directorate of Human Resources, shall ensure that all Secretariat members are notified of this Policy and any relevant supplementary texts and made aware of the matters covered.

3.6. Any contract entered into between an external service provider and the Organisation must make explicit reference to this Policy and the any relevant supplementary texts if access to the Council of Europe's Information System is required for the performance of the contract. This Policy and the supplementary texts must also be brought to the attention of other users.

4. Conditions of use of the Information System

4.1. The Information System may only be used in accordance with the rules set out here and in the supplementary texts, such as the Information Systems Security Policy.

4.2. The Information System is the property of the Organisation. It is intended for the professional activities of users in the Organisation within the limits of their access rights.

4.3. Access rights to the Information System are subject to prior authorisation, which is granted on request to users by the relevant IT department.

4.4. Access rights to the Information System are strictly personal and are subject to authentication. Users agree to respect the limits of their access rights, to protect them and not to disclose their means of authentication or pass them on to a third party, even on a temporary basis.

4.5. In the event of their means of authentication being inadvertently disclosed, users must immediately contact the relevant IT department so that the necessary precautions can be taken.

4.6. Users must not intentionally exceed the limits of their authorised access to files in the Council of Europe's Information System. In the event of unintentional access to such files, they must refrain from using them and contact the relevant IT department.

4.7. Users' access rights must be periodically reviewed by the relevant IT department.

4.8. IT administrators' access rights shall be subject to a request from their direct hierarchical superior and validation by the relevant IT department.

4.9. The access rights granted to IT administrators entail increased duties of care, loyalty, discretion and confidentiality. A security charter sets out the obligations specifically incumbent on them. Any person with privileged access to the Information System, regardless of their relevant IT department, must agree to the charter in writing.

5. Rights and obligations of users

5.1. Any use is subject, according to the status of the person concerned, to compliance with the Staff Regulations and Staff Rules and with the ethical framework, in particular the *Policy on Respect and Dignity in the Council of Europe* and the *Policy on the use of social media by Secretariat members*.

5.2. Users must report any security incident or breach to the entity responsible for information security within the Organisation without delay.

5.3. Anyone who becomes aware of a breach of the provisions of this Policy, or of the supplementary texts, which may constitute wrongdoing is required to report it in accordance with the procedure set out in the Speak Up Policy.

5.4. Personal use of the Information System is acceptable as long as it is reasonable and limited. Such personal use may not, under any circumstances, be considered as a right and is subject, in particular, to the conditions set out below:

- Such use is not incompatible with the aims and values of the Council of Europe, liable to bring the Organisation into disrepute or otherwise prejudicial to it;
- Such use does not affect the work of the user concerned, the work of other users or the security of the Information System;
- All messages and files are protected by the right to privacy and the confidentiality of correspondence, except as provided for in section 6 of this Policy;
- Backing up personal data to professional storage facilities incurs only a marginal cost for the Organisation.

5.5. Users are entitled to the protection of their personal data under the *Council of Europe Regulations on the Protection of Personal Data*. They are responsible for ensuring the protection of the personal data of others when using the Information System.

5.6. Users shall respect the intellectual property rights of the Organisation and third parties.

Use of IT resources

5.7. Secretariat members will be provided with the information and communication technology equipment required for the performance of their duties.

5.8. Users shall be responsible for the proper use of the IT resources provided to them.

5.9. The installation and use of hardware or software on the Organisation's infrastructure or equipment is subject to prior authorisation by the relevant IT department.

5.10. All IT and telecommunications equipment provided by the relevant IT department (e.g. laptops or telephones) must be returned on termination of service.

Internet use

5.11. Internet use via the Information System is controlled by means of a filtering system. DIT or the relevant IT department will, on its own initiative or at the request of the Directorate of Human Resources, block websites which pose a security risk or which appear to be manifestly inappropriate for reasonable use under the provisions of paragraph 5.4 of this Policy.

5.12. Users must not search for, process or send any content which is manifestly unlawful (such as child pornography or religious or xenophobic extremism).

5.13. It is strictly prohibited to access or download via the Information System any content which is manifestly unlawful or which could be prejudicial to the Organisation or to others. It is also prohibited to send via the Information System any electronic communication containing manifestly unlawful content.

5.14. If, on an exceptional basis, access to unlawful content is required for the performance of their duties, the users concerned may access it under their own responsibility. They will be systematically notified and required to certify their need for such access in the light of this paragraph.

5.15. Users may request that DIT or the relevant IT department unblock access to a website referred to in paragraph 5.11 above. DIT or, where applicable, the relevant IT department, shall consider whether the request is justified in the light of the security risks, in consultation, where applicable, with the Directorate of Human Resources.

5.16. Access to social media through the Information System is governed by this Policy and subject to compliance with the provisions of the *Policy on the use of social media by Secretariat members*.

Use of the telephone system

5.17. Personal use of the telephone provided is tolerated as long as it is reasonable.

6. Supervisory and disciplinary measures

6.1. DIT is responsible for ensuring the proper functioning of the Information System. To this end, it must keep the necessary back-ups, archives and logs. The relevant IT departments are entrusted with the same responsibilities within their respective entities. Checks must be

performed to prevent and respond to any attempt to compromise the availability, integrity, confidentiality or traceability of the Information System.

6.2. Surveillance and supervision of the Information System must be carried out in accordance with the principles of necessity and proportionality and, as far as possible, in an anonymous and automated manner.

6.3. Any use of the Information System may be disclosed to the relevant IT administrators, particularly in the event of unreasonable personal usage. Electronic communications and documents marked "private" or "personal" may be subject to the checks set out in paragraph 6.6 of this Policy.

6.4. Impersonalised data is systematically collected during use of the electronic mail system to ensure that the Information System meets requirements (for example, data concerning the size of mailboxes or the total number and volume of messages sent and received).

6.5. In the event of an actual or imminent risk of harm to the Council of Europe's interests or image, such as suspected wrongdoing of such a nature that immediate action must be taken to stop it or to provide an appropriate response, the relevant IT department or the entity responsible for information security within the Organisation may disclose personalised data to the Organisation's competent authorities.

6.6. Targeted and individual checks on the use of the Information System and on the content of any document may be carried out as required in accordance with paragraph 6.1 above, or at the request of a competent authority of the Organisation, either as part of an investigation conducted in accordance with the *Rule on investigations* or for the purposes of co-operation with the national judicial authorities in the context of their proceedings.

6.7. Checks on the content of data collected in accordance with paragraph 6.6 of this Policy will, in principle, be carried out on the basis of keyword searches relating to suspected wrongdoing. Emails and documents labelled as "private" or "personal" will only be subject to digital forensic operations if the aforementioned checks result in the identification of files connected with the subject matter of the investigation.

6.8. No provision in paragraphs 6.1 to 6.7 of this Policy shall be interpreted as adversely impacting the administrative autonomy of the European Court of Human Rights ("the Court") within the Council of Europe and, in particular, the delegation of staff management powers to the Registrar of the Court by the Secretary General,[2] in accordance with Resolution CM/Res(2023)1 establishing the general delegation framework for the Council of Europe Secretariat.[3]

6.9. The relevant IT department has the right – without prior warning – to disconnect hardware or uninstall software installed in breach of paragraph 5.9 of this Policy and that could cause a security incident or impair the proper functioning of the Information System.

6.10. In the event of a security incident or confirmed breach, the relevant IT department may disconnect the affected hardware and temporarily revoke the access rights of some or all

[2] Delegation instrument, signed on 18 September 2024.

[3] Adopted by the Committee of Ministers on 22 February 2023 at the 1457th meeting of the Ministers' Deputies.

users. The users in question shall be duly informed and their access rights restored as soon as possible.

6.11. Users who fail to comply with the rules set out in this Policy and its supplementary texts may have their access rights suspended without prior notice by joint decision of the relevant IT department and the Directorate of Human Resources. The reinstatement of their access rights shall also be subject to such a joint decision.

6.12. Staff members who fail to comply with this Policy or its supplementary texts shall be liable to disciplinary measures commensurate with the nature and severity of the violation, in accordance with Articles 1.5 and 12 of the Staff Regulations. Other users who violate this Policy shall be liable to actions appropriate to their status and the severity of the violation.

7. Final provisions

7.1 This Policy shall enter into force on 1 November 2024. As of that date, it shall repeal and replace *Instruction No. 47 of 28 October 2003 on the use of the Council of Europe's information system*.

7.2 This Policy will be kept under regular review by DIT and the relevant IT departments and may be amended by the Secretary General.

Alain Berset

Secretary General of the Council of Europe

French version signed on 1 October 2024