Code of Conduct for Catalan Institute of Classical Archaeology staff and affiliated staff

Protection of personal data

Instruction 1/2017 of 16 February on the Code of Conduct for the Catalan Institute of Classical Archaeology staff and affiliated staff

This Code of Conduct is the primary instrument of the Catalan Institute of Classical Archaeology for processing and protecting personal data.

Tarragona, 16 February 2017

Institut Català d'Arqueologia Clàssica

1. Code of Conduct

One. Instruction

The need to guarantee the appropriate use of technical, computer and human resources in order to facilitate and expedite the work undertaken at the Catalan Institute of Classical Archaeology (hereinafter ICAC) and ensure compliance with regulations on protecting personal data[1] is an issue of the utmost importance. Therefore, guidelines must be established to raise awareness among the ICAC and affiliated staff[2] with access to these materials in order to ensure the security of computer and communications equipment and all technical and human resources, both inside and outside of ICAC facilities.

All ICAC and affiliated staff with access to data as well as other users with prior authorisation to access data must be familiar with and understand these regulations.[3] Everyone must cooperate in the task of appropriately processing and safeguarding personal data[4] in the performance of their duties. Failure to do so may lead to the imposition of disciplinary measures.

ICAC research associates are excluded from this Code of Conduct, as they do not have access to personal data in the custody of ICAC.

Two. Definitions

This Code of Conduct applies to ICAC and affiliated staff and other users with access to data if they access ICAC technical and computer resources containing data as a result of a commercial, employment or professional relationship.

Three. Objectives

The purpose of this Code of Conduct is to raise awareness among ICAC and affiliated staff of the security of computer equipment, communications equipment and any other material and human resources provided or established inside or outside ICAC premises. The aim of this Code of Conduct is to ensure that these resources are put to good use and to facilitate improvements to the network of communications and relationships in the workplace.

---

[1] Personal data comprises all numerical, alphabetical, graphic, photographic, acoustic or other type of information that identifies or can be used to identify specific individuals. Personal data includes names and surnames, identification card numbers, dates of birth, postal addresses, email addresses, telephone numbers, images (photos and videos), as well as information about appearance, physical traits, bank account numbers, education or studies, professional background, financial situation, social status, etc.

[2] 'ICAC and affiliated staff' includes everyone contracted by ICAC or affiliated with ICAC, with the exception of research associates.

[3] Other users with access to data include companies and professionals authorised to access ICAC data that are obliged to sign a third-party data processing contract.

[4] 'Processing of personal data' means any operation or technical procedure that allows data to be collected, recorded, stored, prepared, processed, modified, consulted, viewed, used, modified, forgotten, blocked or erased, as well as transfer of data in communications, consultations, connections and transfers.

Four. Scope of application

The guidelines set out in this Code of Conduct apply to ICAC and affiliated staff in relation to fixed and portable computer equipment, to all communications made via the external network or internet made available to ICAC and affiliated staff and to all documentation viewed and processed in the course of day-to-day work activities. They apply also to all other instruments and devices used to transmit data over long distances that may be made available to ICAC and affiliated staff.

Five. Processing of personal data

A set of principles related to the nature of the data must be applied in all phases of personal data processing (collection, administration, transfer, processing, etc.).

Data must be kept up to date and must reflect the current status of the individual to whom it belongs[5].

Only data that is appropriate, relevant and does not exceed the scope and purpose for which it is obtained may be collected. In other words, personal data may only be collected and processed when it is absolutely necessary to fulfil its established purpose.

When personal data is collected by means of questionnaires, forms or other similar documents (estimates, invoices, participation in activities, applications, etc.), the individuals from whom the data is collected must be notified. These people must consent[6] to the processing of their data, except in certain exceptional circumstances, for example, if the relationship is a business or contractual relationship.

ICAC has a procedure for the exercise of the rights to access, rectification, cancellation and objection to processing, which it must guarantee within the established terms, conditions and instruments.[7]

To transmit ICAC data to other users with access to data, express authorisation must be requested from the individual in custody of the data file[8] and a contract for data processing on behalf of third parties must be signed.

ICAC and affiliated staff and other users with access to personal data are bound to maintain professional confidentiality.

ICAC and affiliated staff with knowledge of an incident[9] must notify the security officer[10]

[5] This is the natural person who owns the personal data processed.
[6] Consent is deemed to be expression by an interested party of free, unequivocal, specific and informed will allowing the processing of their personal data.
[7] The procedure for exercising the right of access, rectification, cancellation and objection of processing (ARCO rights) is set out in the security document, which can be viewed on the ICAC website or intranet.
[8] ICAC will maintain custody of the data file and will determine the purpose, content and application of processing. ICAC will also guarantee its security, and prevent alteration, loss, and unauthorised access or processing of personal data.
[9] Any anomaly that can affect the data's security, in any domain, whether on paper or in digital format is considered an incident.
[10] The individual responsible for data security will be in charge of coordinating and controlling applicable security measures: the ICAC administrator.

of that incident so an incident record can be maintained. Being aware of an incident and failing to report it is considered a breach of security in the processing of personal data.

The procedure for processing personal data will be provided by ICAC to people with access to data to ensure the data is used correctly.

Six. Processing of files in paper format

Data in paper format processed by ICAC and affiliated staff must comply with certain regulations to ensure the data is used, preserved, archived and transported correctly.

The transfer of documents containing data[11] must be recorded in the entry and exit register, which requires authorisation by the person or entity responsible for the data file – in this case is ICAC. When documentation is transferred, measures must be applied to prevent the misappropriation, loss or unjustifiable access to the data.

Copies and reproductions containing data may only be made by authorised ICAC and affiliated staff with access to computer systems for processing personal data.

Documentation with unnecessary data must be destroyed through appropriate means to prevent access to the data or its recovery. To this end, ICAC and affiliated staff must use the paper shredder authorised for this purpose or destroy documentation in a way that makes it impossible to reconstruct.

Documentation will be kept in secure areas that must remain locked at all times when access to documents with personal data is not required.

Seven. Use of computer systems

ICAC and affiliated staff will be provided with technical and IT resources belonging to ICAC to ensure they can perform their tasks quickly and efficiently.

These resources include computer equipment, applications and systems to facilitate the use of IT tools and email. These resources are not for personal or non-professional use.

ICAC and affiliated staff may not alter any part of the computer equipment or connect it to other systems without prior authorisation of the person responsible for the data file, which is ICAC.

Eight. The use of computer applications and files

General principles

Files and documents in data processing systems must be used for professional purposes only and never for personal or private reasons.

Under no circumstances may personal information be provided to third parties unrelated to professional affairs without the express authorisation of the person responsible for the

[11] Physical transfer of documentation containing data outside ICAC's premises.

data file. ICAC and affiliated staff with access to documents containing personal data must take utmost care to prevent any loss of data.

ICAC may review physical, logical and communications resources for the purpose of technical administration or maintenance tasks required to evaluate performance and usage, and to plan future measures. Access to information kept in these systems must also be safeguarded and ICAC and affiliated staff must be notified of such actions.

Installation of applications

Computer applications installed on computer equipment are the property of ICAC. Using, copying or reproducing these applications for non-professional purposes is prohibited without express approval.

Computer applications may only be installed if ICAC has the appropriate software licences. Installing any type of application without the express consent of the ICAC ICT and Audiovisual Resources Department is prohibited.

Computer applications and file security

As files or applications from unknown sources may introduce viruses into ICAC's computer system, the system's antivirus program will automatically check for viruses in programs and files used on the network. However, because antivirus applications do not completely eliminate the risk of producing and spreading computer viruses, ICAC and affiliated staff should take the utmost care when executing files from unknown sources.

In accordance with law 15/1999, members of ICAC staff[12] are expressly forbidden from accessing computer systems with data belonging to other ICAC staff (username/password), except with express and specific authorisation from the system administrator and the person who uses the computer.

Nine. Use of the internet

All connections and use of computer systems to access public networks such as the internet must be limited to matters directly related to the work of ICAC and affiliated staff in order to ensure the best possible use of IT resources.

Before using information from a network, ICAC and affiliated staff must check whether it is protected by intellectual or industrial property right. If this is the case, use of the information is strictly forbidden.

Ten. Use of email

Computer systems, networks, software and hardware used by ICAC staff are the property of ICAC.

ICAC will provide each ICAC staff member with his or her own individual email address

[12] ICAC staff includes all ICAC and affiliated staff as well as associate staff.

or a general one. This will be done for associate staff on request.

ICAC staff should follow the guidelines set out in instruction 2/2017 of 9 February on ICAC email to ensure the correct use of ICAC's corporate email address.[13]

Those who configure their ICAC email address to link to another account, mobile phone or similar device must notify the ICAC administrator responsible for IT security.

Attached data files from unknown sources should never be opened as they may contain a virus that could damage the ICAC computer system.

ICAC staff should always log off when they have finished using email and should not respond to spam messages or offensive or harassing emails.

Email security

The purpose of these security norms on the use of email is to prevent the possibility of identity misappropriation when using the ICAC email system.

ICAC staff are expressly prohibited from intercepting and/or using corporate email without authorisation.

Termination of employment or professional relationship with ICAC

ICAC staff will have access to ICAC email for the duration of their employment or professional relationship with ICAC. In the event of termination of the employment or professional relationship, access to email will be interrupted after no more than three months. The party responsible for the email, which is ICAC, may access the email account to forward messages of a professional nature to the users it deems appropriate.

Eleven. Confidentiality and duty of secrecy

ICAC and affiliated staff and other users who may have access to ICAC personal data must maintain any confidential information they may become aware of in strict professional secrecy. They must commit to not divulge, publish, transfer, disclose or make this information available to third parties. The duration of this obligation is indefinite and will remain in force after the termination of the employment relationship.

Twelve. Termination of employment or professional relationship with ICAC

ICAC will provide its own and affiliated staff with IT and technical resources to perform their duties for the duration of their employment or professional relationship.

On termination of the employment or professional relationship, ICAC and affiliated staff:

- Must not access computer equipment, files or documents.
- Must return all computer media (computers, laptops, USB memories, CDs, etc.).

[13] Regulations on the use of email may be viewed on the ICAC website or intranet.

- Must leave all files or documents in their custody for professional use unaltered.
- Must delete all personal files under the supervision of the entity responsible for the file, which is ICAC.

Thirteen. Compliance with the guidelines set out in this Code of Conduct

ICAC and affiliated staff must comply with the guidelines set out this Code of Conduct. They must also confirm they are aware of them and commit to adhere to them.[14] Failure to comply with this requirement may lead to disciplinary measures and civil or criminal liability.

2. Consequences of failure to comply with the Code of Conduct

Failure to comply with the obligations set out in this Code of Conduct or the commitment to confidentiality and security in the processing of personal data[15] will constitute an infringement of the regulations on personal data protection and will lead to the imposition of the corresponding penalties in accordance with the gravity of the breach and the principle of proportionality.

Without prejudice to any sanction that may be imposed, ICAC reserves the right to impose any disciplinary and/or corrective measures it deems appropriate in accordance with applicable internal agreements in the employment relationship. Legal action may also be taken in accordance with applicable legislation.

3. Commitment to comply with the Code of Conduct

In accordance with the provisions of current data protection regulations, ICAC will communicate functions and obligations for physical and logical personal data security in its Code of Conduct for ICAC and affiliated staff of ICAC.

Joan Gómez Pallarès
Director

Tarragona, 16 February 2017

[14] ICAC and affiliated staff must sign a commitment document.
[15] ICAC staff must sign this document at the beginning of their relationship with ICAC.