ICAC

Institut
Català
d'Arqueologia
Clàssica

Regulations for the use of ICAC email

Protection of personal data

Instruction 2/2017 of 16 February on the rules governing the use of Catalan Institute of Classical Archaeology email

These email regulations are recommendations for adopting good practices and improving security, especially in regard to data protection.

Tarragona, 16 February 2017

1. Purpose and scope of application

The Catalan Institute of Classical Archaeology (hereinafter ICAC) assigns an institutional email account to each staff member (hereinafter staff member) of ICAC staff, associate staff and affiliated staff, as well as to other users who may need an email account to perform their duties.

This email account is a primary means of communication and allows staff members to communicate with each other both on and off ICAC premises.

It is also the primary method used by ICAC for communications and notifications. It is very important that you check your inbox on a regular basis so you do not miss any important information.

The purpose of this document is:

- To provide a set of criteria to ensure that email is used correctly.
- To inform staff of their obligations with regard to the use of their institutional email account.
- To notify ICAC personnel of the existence of monitoring measures, which are applied only in specific cases and with the minimum level of intervention necessary.

These regulations apply to all personnel who have an email account provided by ICAC. Use of the account implies acceptance of these regulations.

2. General instructions for the use of email

All personnel must use their email in accordance with these regulations.

Anyone with an institutional account is considered a user of ICAC email systems and is responsible for the resources assigned to him or her and for all actions taken using those resources.

Although personal use of email is permitted, it may be monitored by ICAC, with the minimum level of intervention required.

3. Permitted and prohibited uses of email

Use of the email account provided by ICAC should be limited to performing functions related to the institute. Therefore:

- Email may only be used for private purposes if it is used for personal matters and is neither excessive nor detrimental to the security of the institutions computer systems.

- Email may not be used for professional matters unrelated to tasks performed for ICAC or affiliated with the institute.

- In the case of webmail, ICAC will ensure that the company providing the email service has adequate privacy and security policies by means of contractually binding clauses with all parties involved.

- Staff assigned to manage the institute's general email accounts may not use them for personal matters or provide these email addresses for personal matters.

- Email may not be used to contract personal services unrelated to the professional activities of ICAC.

- Configuring email client accounts on ICAC computers other than those provided by the institute is prohibited.

- Using chat programs, social networks, instant messaging, etc. is not allowed during working hours, unless they are related to performing duties assigned by the institute.

4. Inbox management

All staff are responsible for ensuring the information in their email is managed properly. To this end:

- Check and empty your inbox regularly as well as your outbox whenever necessary (in whichever system is used, webmail and/or Outlook) to ensure inboxes do not become overloaded.

- Delete all messages that do not need to be kept. The remaining messages should be filed in the appropriate folder or sub-folder, especially any emails that may have personal content.
- Periodically empty the trash or deleted message folder.
- Only delete messages that are part of administrative procedures and other emails that must be saved from your email account if they have been previously filed in the corresponding folder.
- Designate saved private emails by storing them in a folder specifically for private emails.

5. Use of the addresses published in the ICAC directory

Staff email addresses are published on the institute's website.

These addresses may be used for communications between staff members related to the exercise of their respective duties or those of the institute, as well as by employee representatives.

These addresses may not be provided to third parties outside ICAC unless necessary for the exercise of any of duties entrusted by ICAC or linked to the institute.

ICAC will apply its right of erasure with third parties who improperly use data relating to professional email addresses.

6. Security measures

General measures

As a member of ICAC staff, you must comply with the following security measures.

- Securely safeguard the username and password you use to access your email account and do not share them with any other person.
- Use sufficiently complex passwords that can be easily deduced.

- Do not use the option to save a password to avoid re-entering it each time you connect.

- Block access to your account and computer if you are planning to be absent.

- Do not participate in pyramid message chains.

- Do not disable email filters and security options applied by the system administrator.

- Do not use the preview option.

- Do not open suspicious messages. If you receive a suspicious message, notify the ICAC ICT and audiovisual resources manager immediately.

- Do not send, forward or reply to email messages with sensitive data without prior authorisation of the ICAC security manager, who is the institute's administrator.

- Report all email incidents to ICAC's security officer, who is the institute's administrator.

Electronic signature

Electronic signatures must be used when required to guarantee the authenticity and integrity of emails.

Messages can be signed with an electronic certificate if the following two conditions are met:

- The email sent is associated with a specific person. Electronic certificates can therefore not be used with general email accounts.

- The message is related to the exercise of a person’s duties. The use of electronic certificates for personal and private emails is not allowed.

Encrypted messages

Email messages should be encrypted if they contain:

- Information about ideology, trade union membership, religion, beliefs, racial origin, health or sex life.

- Data obtained for law enforcement purposes without the consent of the individuals concerned.

- Data related to acts of gender violence.

- Other types of data that must be protected.

Password management should be used when using encryption systems with prior authorisation from ICAC. The institute will keep a copy of decryption keys, which will only be used if access to content is required as set out in this policy.

7. Other guidelines for the appropriate use of email

- Use the blind carbon copy (BCC) feature when sending an email message to more than one recipient who is not part of ICAC.

- Use the forwarding option only when the recipient can access the sender of the message, its content and all the information in the chain of emails in it.

- Remove the footer signature when sending a private message from your institutional email address.

- Check recipient addresses before sending a message.

- Delete the addresses of the previous recipients when forwarding an email so as not to inadvertently provide the email addresses of third parties.

- Identify the content clearly and concisely in the subject line.

- Do not include personal data in the subject line.

- Avoid words or expressions that might activate anti-spam programs.

- Check the content of the message before sending it.

- Ensure that the automated footer signature is in keeping with the established corporate model and that an email confidentiality notice is included.

- Organise sent and received messages in folders. Keep your inbox up to date.

- Check the possibility of disclosing the content of attachments before sending them.

- Do not attach files that are too large. If necessary, compress the files or use other computer tools to send large volumes of information.

8. ICAC staff absences

In the event of scheduled staff absences of more than five working days, the email accountholder should activate an out of office or similar message and provide a contact address to ensure the continuity of ICAC activities.

Before leaving, you should save your private information in a personal folder and transfer any information you may need to continue activities during your absence.

9. Termination of relationship with ICAC

ICAC will cancel email service when a staff member’s relationship with the institute terminates or if an accountholder misuses the service. ICAC will keep the email address active for a maximum of three months after termination.

ICAC staff have the right to obtain personal messages currently stored in their personal messages folder. Other messages may be reviewed to ascertain if they are required for business continuity or whether they can be deleted.

10. Off-site email access

When using the email addresses provided by ICAC outside its facilities, the following rules must be followed.

- Do not use the save password option when using shared computers.
- Delete your browsing history and close the browser when you’re finished using it whenever using a shared computer to access webmail.
- Use antivirus software.
- Use the automatic locking function with username and password for mobile devices where corporate email can be used.
- Use encryption for mobile device content.
- Inform the security manager, the institute's administrator, if your corporate email is configured to another account, cell phone or similar device.

11. Access to ICAC email accounts and computers

ICAC may monitor email use to ensure that the system continues to function correctly (volume of traffic, volume of messages sent, etc.).

Access to message content and attached documents will only be allowed when other less intrusive mechanisms cannot be used, and only in the following cases:

- To perform maintenance tasks or tasks related to system security. In these cases, staff will be informed of the scheduled tasks and will be offered the possibility of being present.
- To check, in the context of confidential information or disciplinary proceedings, the use of e-mail, in cases where there are indications of misuse by staff.
- To ensure the continuity of the institute’s activities in the event of unforeseen staff absence.

12. Consequences of failure to comply with these regulations

Failure to comply with the rules and regulations set out in this policy will result in a formal written warning in addition to the adoption of the corresponding disciplinary measures, if applicable.

Joan Gómez Pallarès
Director

Tarragona, 16 February 2017