

## **Rules governing staff access to and use of Parliament's email system**

THE SECRETARY GENERAL,

- having regard to the Staff Regulations of Officials of the European Union (hereinafter 'Staff Regulations') and the Conditions of Employment of Other Servants of the European Union (hereinafter 'CEOS') laid down by Council Regulation (EEC, Euratom, ECSC) No 259/68, as last amended by Council Regulation (EU, Euratom) No 1023/2013, in particular Articles 12, 17 and 17a of the Staff Regulations and Articles 11, 54, 91 and 127 of the CEOS,
- having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data,
- having regard to the Bureau decision of 13 January 2014 on delegation of the powers of the appointing authority and of the authority empowered to conclude contracts of employment (AECE), in particular Article 2 thereof, under which the Secretary-General may adopt staff policy implementing measures,
- having consulted the Legal Service, the Staff Committee and the Data Protection Officer,

Whereas:

- (1) Email is a valuable communication tool whose availability is crucial to the performance of key tasks within Parliament.
- (2) With a view to making sure that the email system performs as efficiently as possible and for purposes of legal certainty, rules need to be laid down governing the use of the system by individual staff members and by the Administration.

- (3) In accordance with their duty of loyalty and their obligation not to engage in conduct unbecoming of their status, users must not send emails that are discriminatory, insulting, persecutory or defamatory to recipients inside or outside Parliament.
- (4) In accordance with their obligation to exercise discretion, officials and other staff members, trainees and accredited parliamentary assistants (hereinafter 'APAs') must not disclose confidential or personal information to unauthorised persons.
- (5) Emails sent by users must not result in major slowdowns in the service.
- (6) It is important to ensure continuity of service when a user leaves the institution. To that end, the user's line manager must be able, after all other avenues have been explored, to obtain copies of the user's work-related emails.

DECIDES AS FOLLOWS:

### **Article 1 - Access to and use of the email service**

1. All officials and other staff members, trainees and APAs (hereinafter referred to collectively as 'users') who are in active service or on leave on personal grounds for a period of no more than six months shall have access to Parliament's email system.
2. Parliament's email system is made available with a view to meeting the needs of the institution and is accordingly intended to be used for professional purposes. It may, however, be used for personal emails within the limits laid down in Article 2.
3. Users must keep personal data and emails in the 'Private' folder made available by Parliament for that specific purpose.

## **Article 2 - Limits on use of the email system**

1. The email system must not be used, either intentionally or through negligence, in such a way as to damage Parliament's interests.
2. No emails that are discriminatory, insulting, persecutory or defamatory may be sent to recipients either inside or outside Parliament.
3. Confidential or personal information may not be disclosed to unauthorised persons.
4. Private use of the email system must remain within sensible bounds and must be in keeping with the rights of third parties, with particular reference to intellectual property rights. Private use of the email system must not, in particular:
  - disrupt Parliament's work;
  - jeopardise the running of the email service;
  - involve any commercial activities;
  - be at odds with the user's contractual obligations or with the Staff Regulations;
  - entail sending emails and attachments to large numbers of recipients simultaneously.

## **Article 3 - Failure to observe these rules**

1. Should the email system be used in breach of these rules, the user's line manager (or, in the case of an APA, his or her Member) shall forward a duly substantiated request to the Director-General of Personnel, who – other than in exceptional circumstances having heard the user concerned – may, for a period of no more than three months:
  - a) restrict the user's access to the email system (for example, by preventing him or her from sending emails) or
  - b) withdraw his or her access to the system altogether.

2. If the Director-General of Personnel decides to take one of the above measures, he or she shall notify the relevant appointing authority, which may open an administrative investigation.
3. In such cases, the Director-General of Personnel's decision shall be notified to the user by registered mail with acknowledgement of receipt or delivered by hand and signed for.
4. DG ITEC shall handle the technical side of implementing the decision to restrict or withdraw the user's access to the system.
5. Complaints may be lodged under Article 90(2) of the Staff Regulations against decisions taken under paragraph 1.

#### **Article 4 - Termination of access and handling of private emails**

1. Users' access to their mailboxes shall be terminated when they leave the service or go on leave on personal grounds for a period of more than six months.
2. Members asking the Administration to terminate the contract of an APA may forward to the Director-General of Personnel a duly substantiated request for the assistant's access to the email system to be withdrawn temporarily, pending the outcome of the enquiries carried out in such cases. If the Director-General of Personnel takes a reasoned decision to withdraw access temporarily, that decision shall be notified to the APA by registered mail with acknowledgement of receipt or delivered by hand and signed for.
3. When users leave the service, they may recover only the private emails they have kept, as required, in their Private folders. To do so, they must submit a request to the Administration within three months of leaving the service. The emails will be sent to them on a storage device such as a CD or DVD.
4. For a period of up to two months after access to a mailbox has been withdrawn temporarily or permanently, anyone sending an email to the mailbox will receive an automatic reply informing them that the user can no longer be contacted at the email address and providing addresses to which emails should be sent.
5. The user may give the relevant department the name of a person to whom

the contents of the Private folder should be sent in the event of his or her death or permanent incapacity. Once the private emails have been returned to the user, or if the user's representative cannot be contacted or one has not been designated, the contents of the mailbox shall be dealt with in accordance with Article 5(1) of these rules. Requests submitted during the retention period by third parties with a legitimate interest shall be dealt with in accordance with Regulation (EC) No 45/2001.

### **Article 5 - Retention of data following termination of service**

1. When a user leaves the service, all his or her emails, including those stored in the Private folder, shall be kept by Parliament for three months. At the end of that period, the emails shall be deleted unless they are the subject of an administrative investigation, a complaint or legal proceedings.
2. Where necessary in order to ensure continuity of service, and after all other avenues have been explored, the user's line managers may obtain copies of all emails other than those in the Private folder. Those copies shall be provided by decision of the Director-General of Personnel in response to a duly substantiated request from the line managers.

### **Article 6 - Protection of personal data**

1. Data relating to use of Parliament's email system shall be processed in accordance with Regulation (EC) No 45/2001.
2. In the event of serious disruption of Parliament's systems, the Secretary-General, or a person duly designated by the Secretary-General, may take a reasoned decision to authorise DG ITEC, on an exceptional basis, to access a mailbox's contents, including the Private folder. Any such action shall not go beyond what is strictly necessary and proportionate in order to restore system and data security and integrity in Parliament.

Before accessing the mailbox's contents, DG ITEC shall inform Parliament's Data Protection Officer and the mailbox's user that it is about to do so. The Data Protection Officer shall be given regular reports on the action taken by DG ITEC.

Submission of those reports may be deferred if one or more of the exemptions or restrictions provided for in Article 20 of Regulation (EC) No 45/2001 apply.

Only DG ITEC staff who have signed a confidentiality declaration may gain access to such data.

3. Users of this IT environment shall be bound by the requirements of Regulation (EC) No 45/2001, in particular the ban on disclosing personal data without due authorisation. They shall also be required to act in accordance with the specific purposes for which the data were collected.

4. Anyone whose personal data are processed shall have the right to access and rectify the data relating to them, on request to the data controller. They may contact the European Data Protection Supervisor at any time ([edps@edps.europa.eu](mailto:edps@edps.europa.eu)).

5. They may also contact the Data Protection Officer ([data-protection@ep.europa.eu](mailto:data-protection@ep.europa.eu)) for further information on the processing of their personal data and on their rights.

### **Article 7 - Entry into force**

These rules will enter into force on the day on which they are signed.

Luxembourg, 7 November 2014

Klaus WELLE