Electronic Mail Policy

Reference:	GMICT P 0090	Publication:	7 November 2025
Version:	3.0	Effective:	7 November 2025

Purpose

To regulate the use of Electronic Mail within Public Administration.

Scope and Applicability

This Policy covers the use of Electronic Mail.

GMICT Policies apply to all users of Government Information Assets, consumers of Government IT services and providers/implementers of Government Solutions.

Definitions

Underlined terms are defined in the **Vocabulary** (GMICT X 0003).

General

1. Data Controllers shall enforce and ensure that their respective Ministry, Department, Secretariat or Entity implements and complies with the General Data Protection Regulation, (EU) 2016/679[1] and the Data Protection Act (CAP 586). Any identified breach shall be reported immediately to the appropriate roles, which include the Data Protection Officer, Data Controller and the Information & Data Protection Commissioner.

2. Account Holders are granted the use of e-mail on behalf of the Data Controller to exchange Official E-mail and to perform activities that are carried out in the public interest, in the exercise of their own official authority or as delegated to them.

   Account Holders should note that their e-mail Account is owned by the Data Controller, who has ultimate authority over its use and over the contents of any associated mailbox.

   An e-mail Account shall not be used by anyone other than the intended Account Holder or delegate working within the remit of the Account Holder's function in Government.

3. A personal[2] e-mail address, including its e-mail prefix, shall be assigned to only one Account Holder within the Public Administration and, upon the Account Holder's expiry, termination, retirement, resignation or dismissal/removal from employment, contractual agreement or assignment, it shall not be reused by, or

[1] The General Data Protection Regulation, (EU) 2016/679 may be found at: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[2] Refers to the address of the Government non-generic email account assigned to the Account Holder for the purposes as established within this Policy.

reassigned to **another** Account Holder. Refer to GMICT Information Security Policy P 0016, '*Account management for specific work life instances*' with respect to reassignment to the **same** Account Holder.

4. A generic e-mail address assigned to an Account Holder may be reused by or reassigned to another Account Holder, subject to the original Data Controller's authorisation.
5. E-mail messages related to Government business shall only be sent or received through an officially corporately provided and recognised e-mail Account.
6. An e-mail address or URL that **is not** officially recognised by the Government, may not be placed on Government stationery or websites.
7. An e-mail address or URL that **is** officially recognised by the Government may not be placed on personal or non-Government stationery or websites.
8. Government e-mail shall not be used for:
    - purposes that are unlawful or constitute a security threat
    - accessing or transmitting Content that is illicit, pornographic or offensive
    - transmitting Spam[3], Counterfeit E-mail or other malicious Content
    - harassment, defamation or disparaging statements
    - infringement of copyright
    - personal gain, private commercial activities or self-promotion
    - any other inappropriate purpose.
9. The Account Holder is responsible for the proper use of the Account. The Account Holder shall ensure that every measure is taken to avoid the possibility of unauthorised access and misuse by others. Apart from this Policy, the Account Holder shall also follow e-mail related guidelines, directives and any other form of formal communication issued from time to time by the Public Administration.
10. Individuals shall not impersonate another Account Holder or any other individual when using e-mail.
11. Account Holders shall only enter into or vary an agreement that legally binds the Government if they are appropriately authorised to do so. In such cases, the Account Holder shall specify that the communication is being sent "without prejudice" to any other statutory or judicial rights that the Account Holder or the Government may have.
12. E-mail Accounts may be granted to non-Government individuals or organisations who have been commissioned to carry out work for or on behalf of the Government, if such a government Account is deemed necessary by the Data Controller to facilitate the fulfilment of this work. The Account shall only be used in pursuance of this work. Such individuals shall adhere to the responsibilities of an Account Holder in terms of this Policy.
13. E-mail Accounts shall not be used for registration to third-party services unless deemed necessary by the Account Holders to facilitate the fulfilment of their work.
14. E-mail messages contending to be originating from any Agent managed domain/s, shall only be generated and sent by the Agent managed infrastructure

[3] Unsolicited junk or bulk E-mail that is not related to work or personal interest.

and not from any other infrastructure or service. Should the latter be necessary, the Agent shall be informed prior to the design or initiation of any related configurations or activities.

15. Connection to the e-mail service shall be made through client software that is authorised and supported, in conformance with the service parameters of their e-mail service provider. The configuration and behaviour of the software are not covered by the e-mail service. The Account Holder is responsible to seek related assistance from the Agent if needed.

16. When a connection to the e-mail service is being done through a device which is not managed by the Agent, the Account Holder shall be responsible for the security of any government data downloaded on that device.

17. The e-mail service shall not be used as a time-sensitive, vital or mission-critical channel, including but not limited to, time-based procurement, vital data transmission, among others. Alternative solutions shall be sought for such requirements.

Logging and auditing

18. All e-mail related activity conducted at any time by the Account Holder is subject to logging and auditing.

19. The Agent shall keep appropriate e-mail activity and audit logs for a pre-determined period of time.

Audits requested by Data Controllers

20. The emphasis of audits requested by Data Controllers, is expected to be on the usage of the e-mail service made by individual Account Holders as well as general performance of the e-mail systems within their respective offices. Based on the audits carried out, the individual Data Controllers may take any action regarding individual Account Holders that they may deem appropriate. This does not exclude any action being taken outside the context of an audit.

21. In cases where the Data Controller or their delegate deems that the e-mail service is being misused, all e-mail Content may be used as evidence in any subsequent investigation and the following actions shall be taken:

    - The Data Controller or their delegate shall inform the Account Holder that their use of the service is deemed to be inappropriate and/or contrary to Government Policy.
    - The Account Holder shall immediately refrain from their misuse of the service on receiving such a communication from their Data Controller. In the event that the Account Holder persists in the abusive behaviour, the Data Controller shall request the Agent to deny the Account Holder access to the relevant service, in order not to jeopardise the integrity of the system or the interests of the Government.
    - The Agent shall carry out an audit if requested by the Data Controller or their delegate.

Audits instigated by the Agent

22. The emphasis of audits instigated by the Agent shall be on the overall usage and performance of the e-mail system, and not on the usage patterns of individual

Account Holders. Based on the audits carried out, the Agent shall advise individual Data Controllers or their delegates on any action it may deem appropriate.

23. In cases where the Agent has a justified suspicion that an e-mail Account is being abused of, it may temporarily disable the Account, informing the Account Holder and Data Controller with reasons why, and may carry out an audit on an ad-hoc basis.

Investigations instigated by other competent authorities

24. In the case of an investigation, the Envelope Information and Content of e-mail messages together with the respective e-mail activity and audit logs, may be disclosed by the Agent to the competent authorities without prior notification to, or consent from, the Account Holder, irrespective of the sensitivity or security classification attributed by the Account Holder to such messages.

User identification

25. Account Holders may not amend any electronic messages received.

26. Account Holders shall not intentionally misrepresent, obscure, suppress, or replace another person's identity on a message received via e-mail, especially when forwarding the message. The sender's name, e-mail address, organisational affiliation, and related envelope or message tracking information included with the message are to remain unchanged.

27. Account Holders shall not send anonymous electronic communications. As a minimum, all Account Holders shall include their name at the end of all electronic communications within their organisation, or a personal signature containing the Account Holder's full name, designation/role, organisation and contact details in formal communications, especially with the public, even when communicating through a generic e-mail Account.

28. E-mail messages sent shall not carry any personalised elements, such as themes and inspirational messages.

29. Account Holders opting to make use of a profile picture, shall ensure that the image used is corporately adequate, and that it may only be used upon authorization from respective management.

30. Account Holders may make use of multiple Mailboxes as required by the Account Holder's business.

31. Multiple e-mail addresses may point to the same mailbox, for example in cases of an Account Holder performing different roles or a change in name through change in marital status.

Signatures

32. The Account Holder shall not amend the e-mail content signature without prior authorization from respective management.

Bulk e-mail

33. Account Holders may send bulk e-mail as required in the execution of their duties, according to the service parameters of their e-mail service provider and subject to the pertinent authorisations.

Out of Office replies

34. It is the responsibility of the Account Holder to perform out of office replies. The Agent shall seek authorisation in writing from the Account Holder or from the respective Data Controller should, in **exceptional circumstances**, out of office replies be required from the back-end.

Auto-forwarding and Redirection

35. Account Holders shall not auto-forward or redirect any incoming e-mail messages to any non-Government mailbox.

36. Account Holders of mailboxes provided by the Agent shall not auto-forward or redirect any incoming e-mail messages to any mailbox that is **not** provided by the Agent.

37. Account Holders shall not auto-forward or redirect e-mail messages from a non-Government e-mail service to any Government mailbox.

38. Account Holders shall not auto-forward or redirect any incoming e-mail messages to any Government mailbox for which they are not responsible without the permission of the Account Holder responsible for the target mailbox.

39. Where auto-forwarding or redirection to Government mailboxes is agreed to by the respective Account Holders, this shall be configured by the end user instigating the auto-forwarding or redirection to facilitate any future investigations that may be required.

40. Auto-forwarding and redirection from the back end shall not be allowed.

Requests for service

41. Account Holders or their delegate shall be responsible to initiate requests for e-mail related services required, in accordance with the service parameters as established by the respective Service Provider.

42. Before sending any request for service to the Agent the requester shall ensure that the request is correctly authorised. In its role as Data Processor, the Agent shall consider all requests to have been appropriately authorised.

Delegation

43. When delegation to a mailbox or mailbox item/s is required, the Account Holder shall assess the least privilege to be given to the delegated person.

44. When the Account Holder delegates access to their mailbox or mailbox item/s, the delegated person, upon its use, shall carry the same responsibilities as the Account Holder and be responsible for their use of the Mailbox.

45. The Account Holder shall ensure that the delegated person is aware of the responsibilities of an Account Holder in this Policy.

46. The Account Holder shall ensure that the delegation is removed when access to the mailbox is no longer required.

Access to an account holder's mailbox (or copies thereof)

47. Account Holders may request from the Agent access to copies of **their own mailbox** and such request shall always be authorised with the written approval of the Data Controller.

48. Individuals may not gain access to, examine, copy or delete **another Account Holder's** e-mail messages, unless such access has been specifically authorised by the Account Holder or Data Controller.

49. Access to the contents of an Account Holder's mailbox, or copies of such mailbox, in order to examine, copy or delete an Account Holder's e-mail messages may only be requested for investigation or business continuity purposes and shall always be authorised with the written approval of the Data Controller. Only the Data Controller shall decide who should be granted access to the Account Holder's mailbox. The Agent shall not accede to requests for access made by other officers. These requests may only relate to any instance in time during which the Account Holder reports to the requester. Under no circumstance shall the Agent interfere with any e-mail message sent from or to any Account Holder's Mailbox, **for the purposes of fulfilling the Account Holder's work**, including, but not limited to, deletion, editing and rerouting.

50. Delivered e-mail messages that are confirmed by the Agent to contain malicious content, and which may therefore constitute a security threat, may be retrospectively auto purged by the Agent.

51. Refer also to the GMICT Information Security Policy (GMICT P 0016), 'E-mail and Internet'.

E-mail address lists

52. The Agent's Global Address List (GAL) and any address lists maintained by the Agent shall only contain official Public Administration e-mail addresses. Such lists shall not be distributed outside of the Public Administration.

53. Address lists maintained by the Agent shall consist of standard Government Ministry, Department, Entity or function names, acronyms or abbreviations.

E-mail Address Structures managed by the Agent

54. An e-mail address managed by the Agent shall be allocated upon a request for service that has been duly authorized by the Data Controller or delegate.

55. In the case of Agent-hosted-domains, the left-hand side of an e-mail address shall be unique, irrespective of the domain.

For personal e-mail accounts[4]

56. The following structures shall apply, according to availability, and may include:

- **name.surname**@Agent-hosted-domain
- **name.*letter(s)*.surname**@Agent-hosted-domain
- **name.surname.*number(s)***@Agent-hosted-domain

For generic e-mail accounts

57. The following structures shall apply, according to availability:

- **name.function**@Agent-hosted-domain[5] *or*

[4] Refers to the Government non-generic e-mail account assigned to the Account Holder for purposes as established within this Policy

[5] For example: survey.opm@Agent -hosted-domain

- **function**@Agent-hosted-domain where the function is a unique function across Government[6].

58. The e-mail address and alias for a generic mailbox shall be agreed by the requesting Government organisation with the Agent prior to communicating or advertising the new generic e-mail address.
59. Names and functions shall be assigned by the Agent on a *first-come-first-served* basis. Any conflict in the use of names and functions that may arise between the requesting organisations shall be resolved between these organisations.
60. The use of special characters within the left-hand side of the address is not recommended. The requestor shall verify with the Agent of any potential technical impact of the use of these characters.

Retention of e-mail and backups

61. It is the responsibility of the Account Holder and Data Controller to ensure that all relevant online and offline e-mail messages are only kept for conducting Government business and/or record purposes, in accordance with legislative requirements, and for no longer than allowed by law.
62. If it is necessary to print e-mail messages and attachments for record purposes, these should be printed together with Envelope Information.
63. The Agent shall only keep backups or copies of mailboxes in line with service parameters. The Agent shall also only keep backups or copies for activity logs for a pre-determined period of time.

Service description

64. Service parameters of the e-mail service shall be made available. It is the responsibility of Account Holders and other relevant stakeholders to refer to them, be aware of their content and abide by them, in accordance with the related contractual agreement.

Maintenance

65. E-mail service maintenance which is anticipated to disrupt service availability shall be planned, in accordance with the service provider's change management policy and/or procedure.

[6] Examples of function are:

- an organisation/entity acronym
- a unique function across Government
- a unique initiative or event

Deviations from GMICT Policy

Instances where it may not be technically possible or cost-effective to comply with a particular GMICT Policy requirement shall be reported as risks at https://rrs.gov.mt to be assessed.

Breaches of GMICT Policy shall be brought to the attention of the respective CIO office in order to determine appropriate corrective action and potential control improvements involving relevant stakeholders, as appropriate.

Issuing Authority

This document has been issued with the authority of the **Principal Permanent Secretary**.

Contact Information

Government ICT Policies and associated publications can be found at **https://ictpolicies.gov.mt**.

Any suggestions, queries or requests for clarification regarding Government ICT Policies, Directives and Standards may be forwarded to **ictpolicies@gov.mt**.