Guideline on the Management of Electronic Messages

Government Records Service
Administration Wing
December 2017 *(with minor updates in November 2020)*

Guideline on the Management of Electronic Messages

Table of Contents

I. INTRODUCTION

Definitions

1. In this Guideline, unless the context otherwise required:

"Electronic address" means a string (any sequence or combination of letters, characters, numbers or symbols of any language) used to specify a source or destination of an electronic message and includes, but is not limited to, an electronic mail address, Internet protocol address, instant messaging account name, telephone number and facsimile number.

"Electronic mail (e-mail)" is an electronic message sent to an e-mail address via a telecommunication system.

"Electronic message" means a message in any form sent over a telecommunications service to an electronic address and includes, but is not limited to, a text, voice, sound, image or video message, and a message combining text, voice, sound, images or video.

"Electronic recordkeeping system (ERKS)" is an information/computer system with the necessary records management capabilities designed to electronically collect, organise, classify and control the creation, storage, retrieval, distribution, maintenance and use, disposal and preservation of records.

"E-mail address" means an electronic address consisting of a user name or mailbox (commonly referred to as the "local part") and a reference to a domain name (commonly referred to as the "domain part"), whether or not displayed, to which an electronic message can be sent.

"Government messaging system" is any information system owned, installed and/or managed by the Government primarily for official business communication through electronic messages. At present, the Government messaging system installed in the majority of bureaux and departments (B/Ds) is capable of sending and receiving e-mail only.

"Record" is any recorded information in any physical format or media created or received by an organisation during its course of official business and kept as evidence of policies, decisions, procedures, functions, activities and transactions.

"Record copy" is the official copy of a record retained for legal, financial, operational, accountability or archival purposes. Only the record copy should be maintained in a recordkeeping system as the corporate information resource.

"Recordkeeping system" is a manual or automated record/information system in which records are collected, organised and classified to facilitate and control their creation, storage, retrieval, distribution, maintenance and use, disposal and preservation.

"Third-party messaging service" is any service for sending and receiving electronic messages provided by a third party. The information system for providing such service is neither owned, installed nor managed by the Government. Examples of third-party messaging services include WhatsApp, WeChat, Facebook, etc. Please see Section VII below for more details.

Purpose and application of the Guideline

2. This Guideline gives guidance and instructions to help B/Ds to identify, create, file and manage electronic message records (including e-mail records) so that adequate and accurate evidence of official business and activities will be retained for operational, policy, legal, financial and archival purposes.

3. This Guideline is intended for Departmental Records Managers, records management staff (including registry staff), all users of electronic messaging (including e-mail) services, Heads of Information Technology Management Units and IT staff (including departmental Local Area Network (LAN) Administrators). As e-mail is commonly used for official communication in the Government of the Hong Kong Special Administrative Region ("Government"), this Guideline will also provide practical guidelines and best practices on the management of e-mail records as one form of electronic message records.

4. At present, while ERKS has been put in place in some B/Ds, it has yet to be fully implemented in the Government for the management of electronic records (including e-mail records). As stipulated in General Circular (GC) No. 2/2009 entitled "Mandatory Records Management Requirements", B/Ds should adopt the "print-and-file" practice to retain e-mail records in their departmental recordkeeping system unless otherwise agreed by the Government Records Service (GRS). This Guideline provides, among other guidance, standardised procedures for the "print-and-file" practice to ensure that the required information of an e-mail record will be adequately and effectively captured in a paper-based recordkeeping system. For ease of reference, a series of flowcharts that illustrates the recordkeeping procedures for different types of e-mail in a paper-based recordkeeping environment is also provided in the Guideline.

II. IDENTIFICATION OF ELECTRONIC MESSAGE RECORDS

Electronic messages as records

5. Record, irrespective of its physical format or media, created or received by a B/D during its course of official business and kept as evidence of policies, decisions, procedures, functions, activities and transactions should be properly captured and managed in a departmental recordkeeping system[1]. In this connection, electronic messages (including e-mail and electronic messages created in short message service (SMS) or other instant messaging services (e.g. WhatsApp, WeChat, Facebook, etc.)) created or received in the course of official business and kept as evidence of such business are records. They are subject to the same legislative and regulatory framework that applies to all other records.

6. To ensure that these electronic message records (including but not limited to e-mail records) are accurately and adequately documented and are readily retrievable and usable as and when required, they should be captured into a reliable departmental recordkeeping system and managed properly.

Rules for identification

7. In deciding whether an electronic message should be treated as a record, the subject officer should make reference to the business rules for records creation and collection of his/her B/D or consult his/her supervisor as appropriate. Whether an electronic message should be treated as a record should not be dependent on its physical format or media. So long as the electronic message should be kept as evidence of policies, decisions, procedures, functions, activities or transactions, it should be captured and managed as a record irrespective of its format and media adopted.

8. Where there is still doubt as to whether an electronic message is a record, the subject officer should consider it a record, and arrange to have it filed in an appropriate manner.

9. Some typical examples of e-mail records and non-records are given in Appendix A.

Features of a complete electronic message record

10. Electronic message records must possess sufficient details of content, context and structure to provide reliable, authentic and complete evidence of official business.

[1] B/Ds should not allow their staff to keep records in personal systems (such as subject officer's desktop computer, shared drive facilities, mailboxes in an e-mail system, etc.) instead of the designated departmental recordkeeping system(s).

11. Content of an electronic message record refers to the information or ideas the record contains. It may be shown in the message body or in the attached document transmitted with the message. Context comprises the information about the circumstances in which the record is created, transmitted, maintained and used. Structure means the physical and/or logical format of the record and the way parts of the record relate to each other.

12. Samples illustrating the content, context and structure of an e-mail record and other electronic messages are given in Appendix B.

Contextual and structural details to be captured

13. To ensure the completeness and reliability of an electronic message record, in addition to its content, B/Ds should capture the following contextual and structural details as far as possible:

a. Details of the author (including the author’s full name, designation, organisation name and electronic address (i.e. e-mail address for an e-mail record));

b. Details of the recipient(s) (including the recipient’s full name, designation, organisation name and electronic address (i.e. e-mail address for an e-mail record));

c. Transmission and receipt information including date and time of sending and receiving the electronic message;

d. Subject or title of the electronic message;

e. File reference of the electronic message if a copy of it will be filed as a record;

f. Security grading where applicable; and

g. Indication of any attached document and its filename.

III. FILING[2] OF E-MAIL RECORDS

14. As e-mail is one type of the commonly used electronic messages for official communication in the Government, the ensuing paragraphs will provide practical guidelines and best practices on the management of e-mail records as one form of electronic message records.

[2] Filing is a process in which responsible staff analyse the content of a document, classify it according to established records classification scheme, and capture it in B/D’s designated paper-based recordkeeping system or ERKS. Effective filing contributes to prompt, accurate and complete retrieval of information.

The filing responsibility

15. To ensure that the record copy of an e-mail record is captured in the recordkeeping system, B/Ds are suggested to adopt the following rules in their business rules for creation and collection of records:

a. Where the sender and recipient(s) of an e-mail record are using the same file, the sender should designate his/her copy as the record copy and arrange to have it filed in the recordkeeping system; and

b. Where the sender and recipient(s) of an e-mail record are using different files (for example, communication between a bureaux and a department or with outside organisations or individuals), the action officer should arrange to have his/her copy filed.

Filing options

16. There are two options for filing e-mail records:

a. Electronic filing – capture e-mail records to an ERKS for management in a consistent and integrated manner; or

b. Print-and-file – print e-mail records and file the printout in a paper-based recordkeeping system.

Electronic filing by ERKS

17. ERKS offers an effective and long-term solution to the management of electronic records in a hybrid records management environment. With the growing need for proper management of electronic and non-electronic records in a consistent and integrated manner, it is the Government's records management policy to pursue electronic records management (ERM)[3] in B/Ds. Under the Government's ERM policy, B/Ds should develop or adopt an ERKS according to GRS' prescribed requirements to drive ERM in the Government. B/Ds with an ERKS implemented in their organisations and with the agreement of GRS will adopt electronic filing instead of the "print-and-file" practice set out below.

Print-and-file

18. Unless otherwise agreed by GRS, B/Ds should adopt the "print-and-file" practice for managing their e-mail records, i.e. subject officers should arrange to print the e-mail records and put the hard copy on paper files similar to other paper records.

The role of the subject officer

[3] More details on ERM concepts, standards and best practices are available on the ERM theme page on the Central Cyber Government Office (CCGO) at http://grs.host.ccgo.hksarg/erm/.

19. The subject officer should confirm the record status of the e-mail sent or received through his/her mailbox, arrange to print the e-mail record and attachment (if any) and pass them to the registry staff for filing.

20. The subject officer or his/her delegate should check and ensure that sufficient details of the content, context and structure of the e-mail record have been printed or manually marked on the printout (see paragraph 13).

21. The subject officer should arrange to:

a. Print the e-mail record for filing as soon as possible upon its transmission or receipt in accordance with his/her departmental records management policy and business rules for creation and collection of records. Under normal circumstances, e-mail records should be printed and filed within 30 days upon transmission/receipt and under exceptional circumstances, e-mail records could be printed and filed within three months;

b. Print the e-mail record directly from the e-mail client program. To preserve record authenticity, the e-mail record should not be exported or copied to other programs for printing;

c. If the time of transmission or receipt of the e-mail record is critical to the transaction, check the correct time on the e-mail server;

d. Where operationally required, identify the full name and designation of the recipient(s) and manually mark such details on the printout; and

e. Store multimedia or non-textual attachments that cannot be printed out to an appropriate storage medium (e.g. removable storage medium the content on which cannot be changed or a designated directory on the server which is configured read-only to authorised users)[4]. To facilitate cross-referencing, there should be an index showing the details of the attachments stored on those storage media and the file reference of the corresponding e-mail message.

The role of the registry staff

22. Similar to the handling of other paper records, registry staff should classify, index and code the printout of e-mail records without delay.

[4] When selecting the storage medium, B/Ds should take into account the access control and security requirements as appropriate. B/Ds should also implement suitable measures to preserve such electronic records from technology obsolescence, media fragility and physical damage. Please refer to the ***Handbook on Preservation of Electronic Records*** for more details on preservation of electronic records (http://grs.host.ccgo.hksarg/erm/s04/461.html).

23. Registry staff should ensure that all the necessary information is printed or manually marked on the printout and that all attachments, if any, are filed with the message in processing such records. Where there is doubt about the completeness of the record, advice from the subject officers should be sought.

IV. Filing of Electronic Message Records other than E-mail Records

24. The principles, guidelines and procedures given in paragraphs 15 - 23 of this Guideline are also applicable to electronic message records other than e-mail records. In other words, electronic message records should either be captured into an ERKS directly or be printed-and-filed in a paper-based recordkeeping system as soon as they are transmitted or received (for example within the next two working days). In particular, the subject officer should ensure that sufficient details of the content, context and structure of the electronic message record have been printed or manually marked on the printout as listed in paragraph 13.

25. B/Ds should note that on occasions where an electronic message cannot be directly captured into a departmental recordkeeping system (such as an interface with B/Ds' ERKS or a "print" function is unavailable when using a third-party messaging service (please also refer to paragraphs 45 - 47 below for more information)), alternative options such as documenting the details of the discussion and/or decision process through the departmental e-mail system or using other acceptable means to document the details of the discussion and/or decision process should be considered[5]. No matter what kind of acceptable means have been adopted for capturing the electronic message record, B/Ds should ensure that sufficient details of the content, context and structure of the electronic message record are available, and that the relevant practices and procedures should be properly documented and promulgated in such a way that can be used by staff in their daily work.

26. For example, if the subject officer of a B/D has adopted third-party messaging services (e.g. WhatsApp, SMS, etc.) for internal communication with his/her colleagues or external communication with external parties, he/she should capture those WhatsApp or SMS messages which are identified as records according to the B/D's business rules for records creation and collection into the B/D's subject file or subject folder in an ERKS. In this case, given that the electronic messages especially those created through third-party messaging services are often very short and lack the necessary contextual information in the message content, the subject officer should document a note of the discussion on the subject file or subject folder in an ERKS in accordance with the departmental business rules for records creation and collection (please also see paragraph 25 above for options to document the details

[5] In the case where technical solutions are considered not feasible or cost-effective by a B/D for capturing electronic message records directly or indirectly into a departmental recordkeeping system, subject officers may follow departmental business rules for creation and collection of records to document a note of the discussion on the paper file or in the ERKS.

of the discussion where an electronic message cannot be directly printed out or captured into a departmental recordkeeping system).

V. APPROPRIATE USE OF THE GOVERNMENT MESSAGING SYSTEM

27. The Government messaging system is installed primarily for official business communication. At present, the Government messaging system installed in the majority of B/Ds is capable of sending and receiving e-mail only (but not other types of electronic messages). Such messaging system for sending e-mail only may also be referred to as an e-mail system.

28. Although Government policy permits officers to send and receive personal electronic messages using the Government accounts provided via the Government messaging system, extensive use of the system for private communication that may interfere with the normal work activities should be avoided. To protect themselves against phishing attacks and malware infections when using e-mail, officers should not use official e-mail accounts for private communication or activities, in particular with external parties. Comments or materials that are illegal, inappropriate, offensive or disrespectful to others should not be disseminated through the system.

29. Disciplinary proceedings may be considered against those officers who have infringed the Government's policy or guideline on the use of Government messaging system, or related regulations or instructions issued by relevant authorities, subject to the gravity and consequence of such infringement.

Segregation of official and personal electronic messages

30. To facilitate proper management of electronic message records, officers should avoid mixing official and personal messages in their individual account (where applicable). Officers should remove and delete personal messages from the account (where applicable) as soon as possible.

Privacy of personal electronic messages

31. The Government does not guarantee privacy of personal electronic messages sent or received via the Government messaging system, nor will the Government be held responsible for such messages. It reserves the right to access all electronic messages sent or received via the Government messaging system where circumstances warrant or for the purpose of, for example, system maintenance, guarding against unlawful activities or abusive behaviour.

32. When an officer has inadvertently been given access to another officer's personal message(s) as a result of a message(s) being wrongly sent to him/her, he should inform the sender as soon as practicable and should not disclose the information in the personal message(s) to a third party without the consent of the data

subject.

Ownership of Government electronic message records

33. Official electronic message records are Government property and the Government has the right to access, read, use, manage and dispose of these records. Some electronic message records may also be selected as archives for permanent preservation.

Regulatory requirements for electronic message records

34. Like all other Government records, electronic message records are subject to the requirements of laws and regulations such as the Evidence Ordinance, Copyright Ordinance, Official Secrets Ordinance, Personal Data (Privacy) Ordinance, Electronic Transactions Ordinance, Unsolicited Electronic Messages Ordinance, Limitation Ordinance, Code on Access to Information, Security Regulations (SR) and Public Records (Access) Rules 1996, etc.

35. It should be noted that unknown, incomplete, unmanaged or mismanaged electronic message records that are subsequently unusable, inaccessible, irretrievable or released to unauthorised individuals would expose the Government to legal, business and accountability risks.

Copyrighted materials

36. Copyrighted materials, including those downloaded from the Internet[6], should not be stored in the Government messaging system or disseminated to others without the prior permission of the relevant copyright owners.

Creation control of e-mail records

37. To ensure efficient and cost-effective records management, officers should create e-mail to meet operational, policy, legal and financial purposes. Officers should also take note of the circumstances in deciding whether communication by e-mail or paper is more appropriate. In general, using one mode of communication, and preferably the same mode adopted by the sender, in making a reply would suffice.

Composing e-mail records

38. Officers resorting to e-mail communication via the Government messaging system represent the Government, as is the case when they communicate by paper correspondence. Officers should use appropriate tone and wording, and carefully check their e-mail and attachments for proper content and tone before transmission.

[6] Software from the Internet should not be downloaded to run on a government computer without permission of the copyright owner and the Head of B/D. For details, please see OGCIO Circular No. 3/2008 – "Intellectual Property Rights Protection through Proper Management and Use of Software".

39. Officers should not put the text all in capital letters as it will make the text difficult to read. Moreover, uppercase text is often interpreted as having extra emphasis.

40. Officers should preferably limit an e-mail message to one subject matter and assign a brief but meaningful title in the "Subject" field for easy identification.

41. To facilitate filing and information retrieval, officers should give adequate information about the e-mail in the body of the message as listed in paragraph 13.

42. e-Memo templates have been tailor-made for B/Ds to standardise the layout of Government e-mail records and ensure that the required details are properly captured. e-Memo templates should be used when issuing memo in electronic form via the e-mail system (where applicable).

VI. INFORMATION SECURITY IN RELATION TO THE GOVERNMENT MESSAGING SYSTEM

Responsibilities of B/Ds

43. B/Ds are responsible for applying adequate security measures to their business routines and protecting Government information and computer resources, including electronic message records and the messaging system, against internal and external fraud and unauthorised access.

Related regulations and guidelines

44. In dealing with security issues relating to information systems and classified information in electronic form, B/Ds should follow the provisions set out in SR, Baseline IT Security Policy (S17), B/Ds' departmental IT security policy, IT Security Guidelines (G3), Office of the Government Chief Information Officer (OGCIO) Circular No. 4/2017 entitled "Practice Guide on the Use of Electronic Mail" and other information security requirements and guidelines issued by the Government.

VII. USE OF THIRD-PARTY MESSAGING SERVICES

45. As mentioned in paragraph 27 above, the Government messaging system installed in the majority of B/Ds is only capable of sending and receiving e-mail. B/Ds may, in consideration of their business, operational and records management needs, adopt third-party messaging services (e.g. WhatsApp, WeChat, Facebook, etc.) for conducting their official businesses. B/Ds should in particular note that the electronic messages created or received using these services may be stored on servers

of the service provider instead of on Government servers. As such, SR and other relevant regulations, instructions and guidelines must be fully complied with. In addition, B/Ds should note that the long-term availability of those electronic messages kept on third-party servers for capturing as official records may not be guaranteed. If B/Ds, after due consideration, still consider that there is a need to adopt third-party messaging services for internal and/or external communication, they should capture those electronic message records to their departmental recordkeeping system as soon as possible (for example within the next two working days) in accordance with their departmental records management policy and business rules for creation and collection of records. As mentioned in paragraph 5 above, only those electronic messages created or received for official business and kept as evidence of such business should be captured as records.

Use of privately-owned devices and accounts

46. If third-party messaging service is adopted by a B/D, electronic message records should normally be created using Government accounts and Government devices. Officers are advised not to use their privately-owned devices or accounts for official communication. If privately-owned device or account is used for third-party messaging service under urgent circumstances[7], the officer concerned should capture those electronic message records to his/her departmental recordkeeping system as soon as possible (for example within the next two working days) in accordance with their departmental records management policy and business rules for creation and collection of records. At the same time, the officer concerned should also observe the relevant requirements governing the storage, processing and transmission of classified information stipulated in paragraphs 34 and 44 above.

Creation of electronic message records

47. Given the nature of instant messaging services on different social media, electronic messages created through such services are often very short and lack the necessary contextual information in the message content. Officers should therefore take note of the circumstances in deciding whether communication by such services or by e-mail is more appropriate.

[7] According to OGCIO Circular No. 4/2017 entitled "Practice Guide on the Use of Electronic Mail", private Internet e-mail service (including webmail) should not be used for official communication unless authorised by Head of B/Ds, in particular when communicating with the public in official capacity.

VIII. DISPOSAL[8] OF ELECTRONIC MESSAGE RECORDS

Destruction of the record copy

48. As is the case of paper records, B/Ds should, based on their operational, policy, legal and financial requirements, compile and agree with GRS their records retention and disposal schedules for electronic message records; and comply with the mandatory requirements as stipulated in GC No. 2/2009, including seeking the endorsement of a senior officer not below the rank of Senior Executive Officer or equivalent in the B/D and obtaining the prior agreement of the GRS Director before permanent erasure or destruction of the record copy.

Deletion of the electronic copy after filing

49. In general, after the printout of the electronic message record has been captured into a recordkeeping system, the electronic copy, which is no longer a record, can be deleted from the subject officer's account (where applicable) within such period as considered appropriate by the concerned B/D taking into consideration any housekeeping requirement as mentioned in paragraph 51.

Destruction of non-records

50. Non-records such as the duplicate electronic version of electronic message records as mentioned in paragraph 49, convenience or reference copies of electronic message records and personal messages can be disposed of without separate agreement of the GRS Director.

Regular housekeeping

51. The Government messaging system must not be used as a storage area for files and documents. The departmental LAN Administrator should ensure that old electronic messages would be purged periodically and automatically.

Transfer of archival electronic message records to GRS

52. B/Ds should transfer those electronic message records appraised by GRS as possessing archival value to GRS for permanent retention. For those electronic message records which cannot be fully captured by the "print-and-file" approach (e.g. those e-mail records with multimedia or non-textual attachments which have been stored on appropriate storage medium such as CD-ROM), B/Ds should contact the Public Records Office of GRS for details on transfer of such records with archival

[8] Disposal is actions taken with regard to records as determined through the appraisal of legal, financial, operational, accountability and historical values of the records. Disposal actions may include physical destruction or permanent erasure of records of no residual value, transfer of records to GRS for inactive storage for a specific period before destruction/erasure, or transfer of records appraised to have archival value to GRS for permanent retention.

value to GRS.

IX. MANAGEMENT OF CLASSIFIED E-MAIL RECORDS

Transmission of classified e-mail

53. Confidential Mail Systems (CMS) are installed for Government internal communication of classified information. At present, CMS include the "CONFIDENTIAL MAIL SYSTEM" (CMS plug-in solutions), "CONFIDENTIAL MESSAGING APPLICATION" (CMSG) and "MOBILE CONFIDENTIAL MAIL SERVICE" (MCMS).

54. CMS are designed for B/Ds to transmit classified documents up to CONFIDENTIAL level via the Government Communication Network (GCN). Other systems that conform to the requirements stipulated in SR may also be used to transmit RESTRICTED information via GCN. For example, RESTRICTED e-mail records can be sent using Lotus Notes via GCN .

55. Before using CMS to transmit classified records, officers must be equipped with the necessary facilities. In addition, officers should make sure that the recipient(s) are registered CMS users and the "Subject" and "File Reference" fields of the message to be transmitted do not contain classified information.

56. At the moment, CMS are the only means by which officers can transmit CONFIDENTIAL e-mail via GCN.

Printing and handling of RESTRICTED and CONFIDENTIAL e-mail records

57. In addition to the procedures given in paragraphs 18 - 23 of this Guideline, the subject officer or his/her delegate should only use a local printer or remote printer in a trusted network to print RESTRICTED and CONFIDENTIAL e-mail and attachments. Other requirements in SR, S17 and G3 should also be observed.

58. Registry staff should classify and put the printout of security graded e-mail records on paper files that have the same or higher security classification of the records, and strictly follow SR in handling different security graded documents.

59. Multimedia or non-textual RESTRICTED and CONFIDENTIAL attachments that cannot be printed out should be stored on an appropriate storage medium in compliance with SR and S17. For example, classified information must be encrypted during storage.

Destruction or erasure of RESTRICTED and CONFIDENTIAL e-mail records

60. B/Ds should follow the requirements stipulated in SR in disposing of or erasing RESTRICTED and CONFIDENTIAL e-mail records. B/Ds should refer to

G3 for technical details.

61. B/Ds should comply with the mandatory requirements as stipulated in GC No. 2/2009, including seeking the endorsement of a senior officer not below the rank of Senior Executive Officer or equivalent in the B/D and obtaining prior agreement of the GRS Director before any classified e-mail records are destroyed or permanently erased. Paragraphs 48 - 52 of this Guideline also apply to the disposal of classified e-mail.

Related regulations and guidelines

62. In addition to SR, B/Ds should also refer to the most up-to-date guidelines and manuals issued by OGCIO on matters relating to system operation, administration and security.[9]

[9] Related OGCIO's guidelines include guidelines on the Download and FAQ pages of CMS Plug-ins Theme Page (http://cms.host.ccgo.hksarg/index.htm) and CMSG and MCMS Theme Page (https://itginfo.ccgo.hksarg/content/ngci/cmsg/index.html) on ITG InfoStation.

Appendix A

Examples of E-mail Records and Non-records

Typical examples of e-mail records:

- Correspondence relating to formulation and execution of policies and operating procedures
- Commitments, decisions or approvals for a course of action
- Documents that initiate, deliberate, authorise or complete business transactions
- Work schedule and assignments
- Agenda and minutes of meetings
- Drafts of major policies or decisions circulated for comments or approval
- Final reports or recommendations
- Documents of legal or financial implications
- Acknowledgements of receipt of e-mail records that document essential transactions

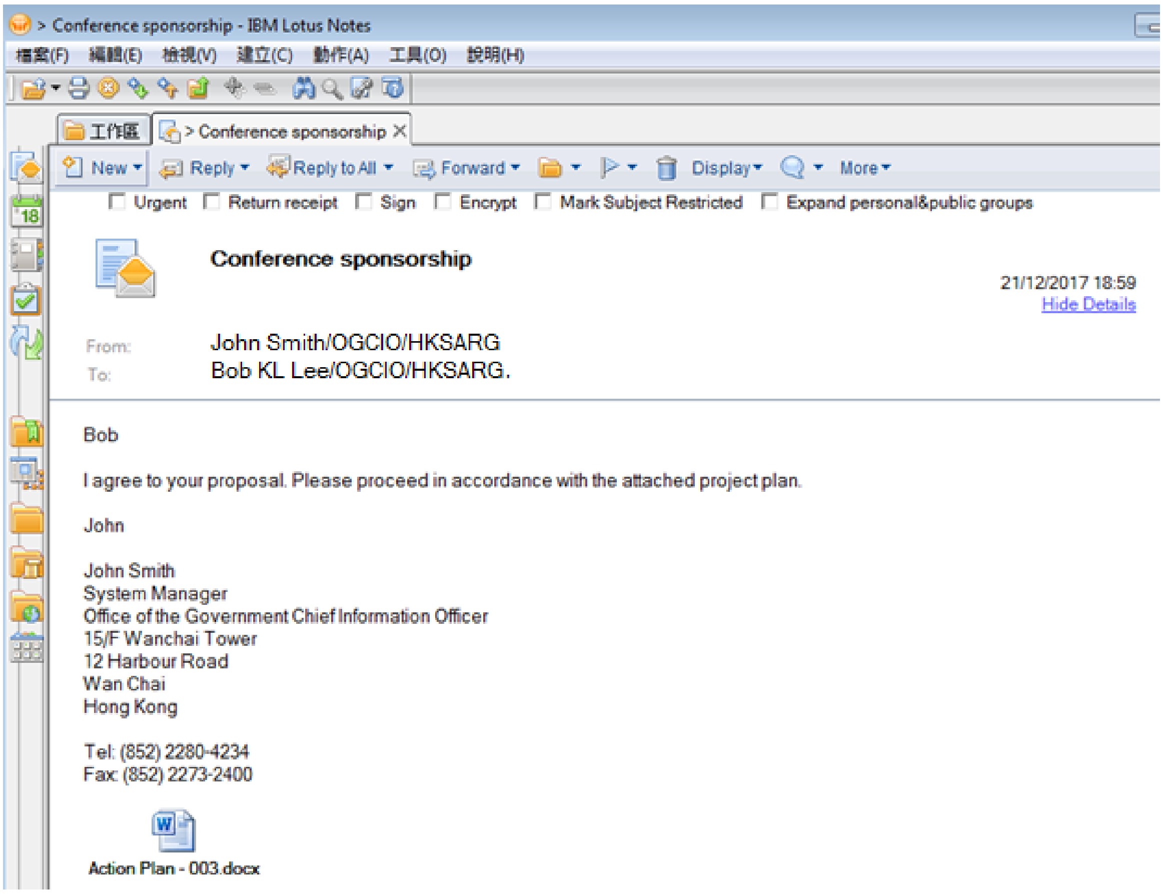
Typical examples of non-records:

- Messages of personal nature
- Copies or extracts of documents that are published or downloaded and distributed for information or reference purposes
- Phone message slips
- Electronic copy of an e-mail record of which the record copy has been filed

Features of Electronic Message Records

(1) An e-mail record

A sample illustrating the content, context and structure of an e-mail record is given below:


> Conference sponsorship - IBM Lotus Notes
檔案(F) 編輯(E) 檢視(V) 建立(C) 動作(A) 工具(O) 說明(H)
工作區
> Conference sponsorship
New
Reply
Reply to All
Forward
Display
More
□ Urgent □ Return receipt □ Sign □ Encrypt □ Mark Subject Restricted □ Expand personal&public groups
Hide Details
18

Conference sponsorship

21/12/2017 18:59

From: John Smith/OGCIO/HKSARG
To: Bob KL Lee/OGCIO/HKSARG.

Bob

I agree to your proposal. Please proceed in accordance with the attached project plan.

John

John Smith
System Manager
Office of the Government Chief Information Officer
15/F Wanchai Tower
12 Harbour Road
Wan Chai
Hong Kong

Tel: (852) 2280-4234
Fax: (852) 2273-2400

Action Plan - 003.docx

Content:
Content refers to the information or ideas the record contains. It may be shown in the message body or in the attached document transmitted with the message.

In the above example, content refers to the message, "I agree to your proposal. Please proceed in accordance with the attached project plan". The content also refers to the content of the attachment "Action Plan - 003.docx".

Context:
Context comprises the information about the circumstances in which the record is created, transmitted, maintained and used.

Context can be addressed at many different levels. In the example above, the context is the e-mail address information in the "To" field, the subject (viz. "Conference sponsorship") and the information in the body indicating that the message is being sent to "Bob" from "John" (for which there is some identifying information such as position, address, etc.). The context is also the information at the bottom of the message that there is an attachment, "Action Plan - 003.docx". Other contextual information also exists which may be hidden from view or that may not emerge until after the message has been sent (e.g. date).

Structure:
Structure means the physical and logical format of the record and the way parts of the record relate to each other (for instance, the message header and the message body; the message body and its attachments).

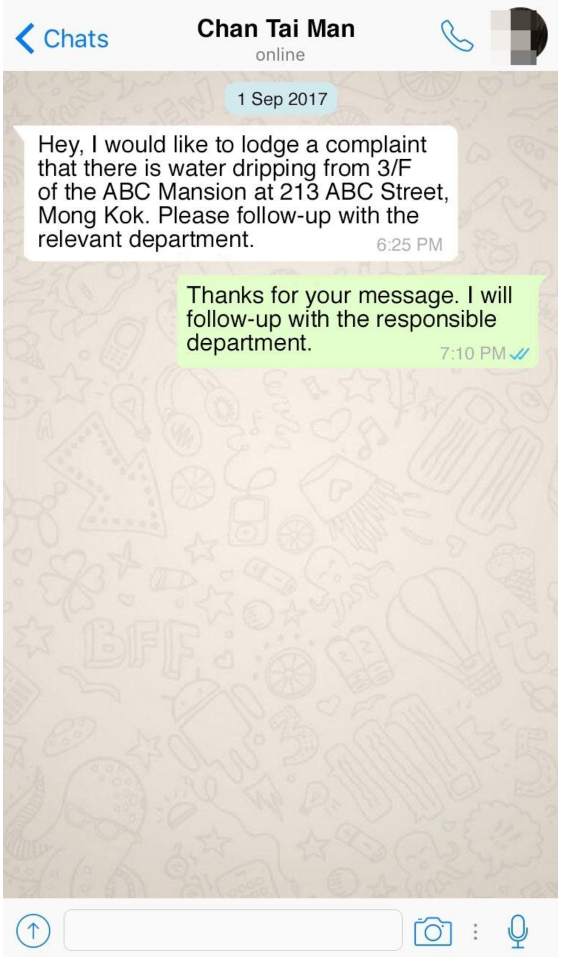
In the example above, the structure would comprise all of the elements that make up the documentary form of the e-mail message. These would include the header fields (not the information in the fields, only the headers themselves such as "to", "from", "subject", etc.), the length of the fields, their position on the message, etc. Also included would be the format of the message body and the identifying link to attachments (but not the contents of the attachment itself). Anything that would comprise the layout and format of the message would be considered to form its structure.

Filing of e-mail record

The subject officer should capture those e-mail records by adopting the "print-and-file" practice to keep them in B/D's paper-based recordkeeping system or capture them directly in the B/D's ERKS where available.

(2) <u>An electronic message record other than e-mail record</u>

As the layout of an electronic message other than an e-mail will be different depending on what type of third-party messaging services and devices are used, a sample illustrating the content, context and structure of a typical electronic message record is given below:



1 Sep 2017

Hey, I would like to lodge a complaint that there is water dripping from 3/F of the ABC Mansion at 213 ABC Street, Mong Kok. Please follow-up with the relevant department. 6:25 PM

Thanks for your message. I will follow-up with the responsible department. 7:10 PM ✓✓

Content:
Content refers to the information or ideas the record contains. It may be shown in the message body or in the attached document transmitted with the message.

In the above example, content refers to the chain of conversation including the first message, "Hey, I would like to lodge a complaint that there is water dripping from 3/F of the ABC Mansion at 213 ABC Street, Mong Kok. Please follow-up with the relevant department." and the subsequent response, "Thanks for your message. I will follow-up with the responsible department."

Context:
Context comprises the information about the circumstances in which the record is created, transmitted, maintained and used.

Context can be addressed at many different levels. In the example above, the context is the name of contact person (viz. "Chan Tai Man") in the conversation and the information in the body indicating that a message was received from a "Chan Tai Man" at 6:25 pm and a response was sent to "Chan Tai Man" at 7:10 pm by the recipient. The context is also the information that the message and the response were sent on 1 September 2017. Depending on the interface of the third-party messaging service, the contextual information of the date in an ongoing conversation may be hidden from view or the date may not be shown specifically (e.g. the system may show "Today" instead of the exact date). Other contextual information also exists which may be hidden from view (e.g. name of recipient of the electronic message). Some contextual information may not be available (e.g. the subject, sender's position and organisation name, recipient's post and organisation name, file reference, security grading).

Structure:
Structure means the physical and logical format of the record and the way parts of the record relate to each other (for instance, the message header and the message body; the message body and its attachments).

In the example above, the structure would comprise all of the elements that make up the documentary form of the electronic message. These include the header field (not the information in the field, but only the sender's name field), the date fields of the electronic messages and their positions in the conversation, the position of the electronic messages in the conversation, etc. If the conversation includes any attachment, the structure that would be included is the identifying link to attachment (but not the content of the attachment).

Filing of electronic message records other than e-mail

The subject officer should capture those electronic messages which are identified as records according to the B/D's departmental business rules for creation and collection of records. Given that the electronic messages especially those created through third-party messaging services are often very short and lack the necessary contextual information in the message content as illustrated above, the subject officer should ensure that sufficient details of the content, context and structure of the electronic message record are retained for operational, policy, legal, financial and archival purposes.

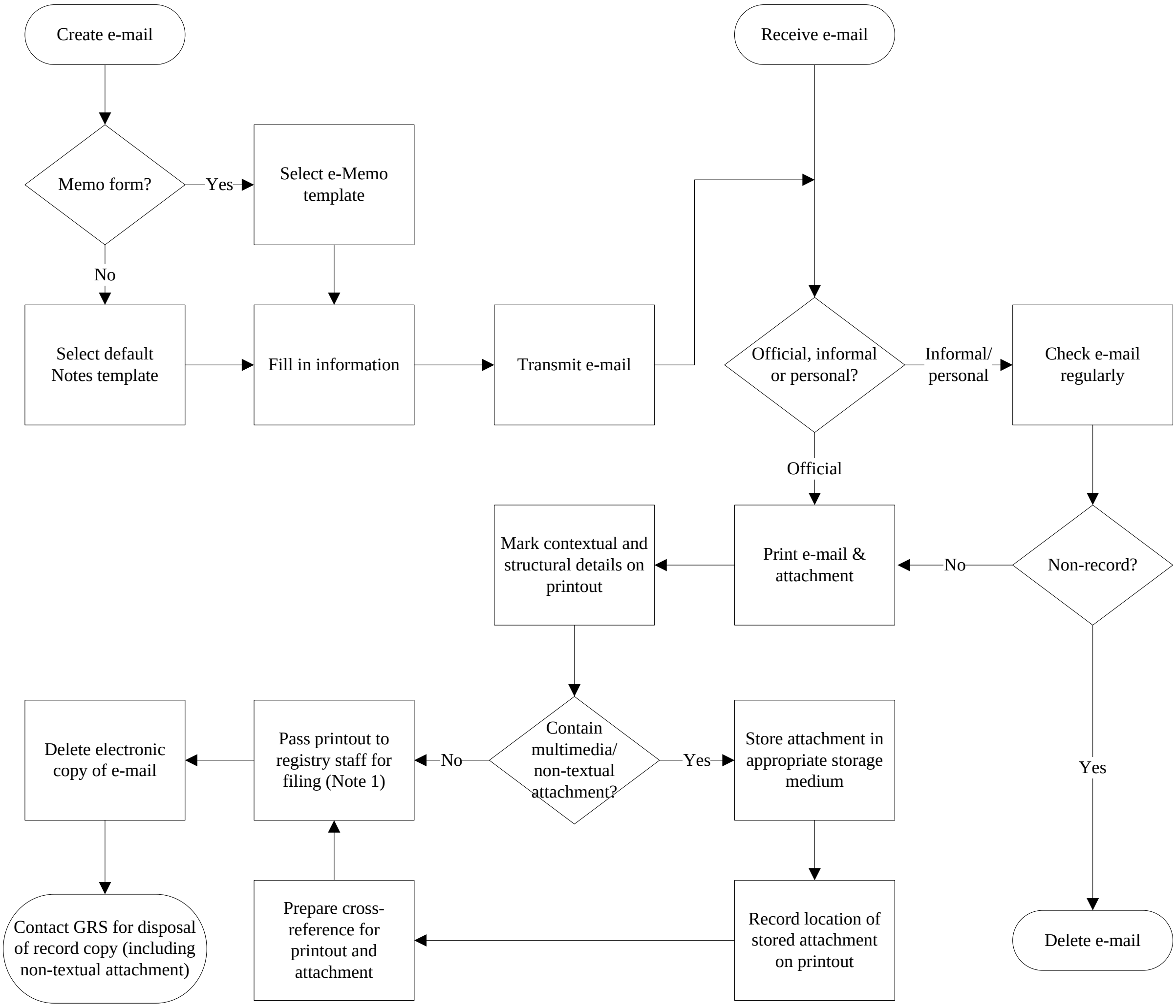
The subject officer should capture the electronic message records into an ERKS directly or print-and-file the records and put them in a paper-based recordkeeping system (if the concerned B/D has not yet implemented an ERKS) and mark the essential context of the electronic message record on the printout. On occasions where an electronic message cannot be directly captured into a departmental recordkeeping system e.g. due to the lack of a "print" function or other technical constraints of the third-party messaging service, the subject officer should consider adopting the following alternative options:

a. document the details of the discussion and/or decision process through the departmental e-mail system and capture it into a departmental recordkeeping system; and/or

b. document a note of the discussion and/or decision process on the B/D’s subject file (or in the ERKS where available).

Flowchart 1

Create and Handle Unclassified E-mail



Create e-mail
Memo form?
Yes
No
Select e-Memo template
Select default Notes template
Fill in information
Transmit e-mail
Receive e-mail
Official, informal or personal?
Informal/ personal
Official
Check e-mail regularly
Non-record?
No
Yes
Print e-mail & attachment
Mark contextual and structural details on printout
Contain multimedia/ non-textual attachment?
No
Yes
Store attachment in appropriate storage medium
Pass printout to registry staff for filing (Note 1)
Delete electronic copy of e-mail
Contact GRS for disposal of record copy (including non-textual attachment)
Prepare cross-reference for printout and attachment
Record location of stored attachment on printout
Delete e-mail

Note:

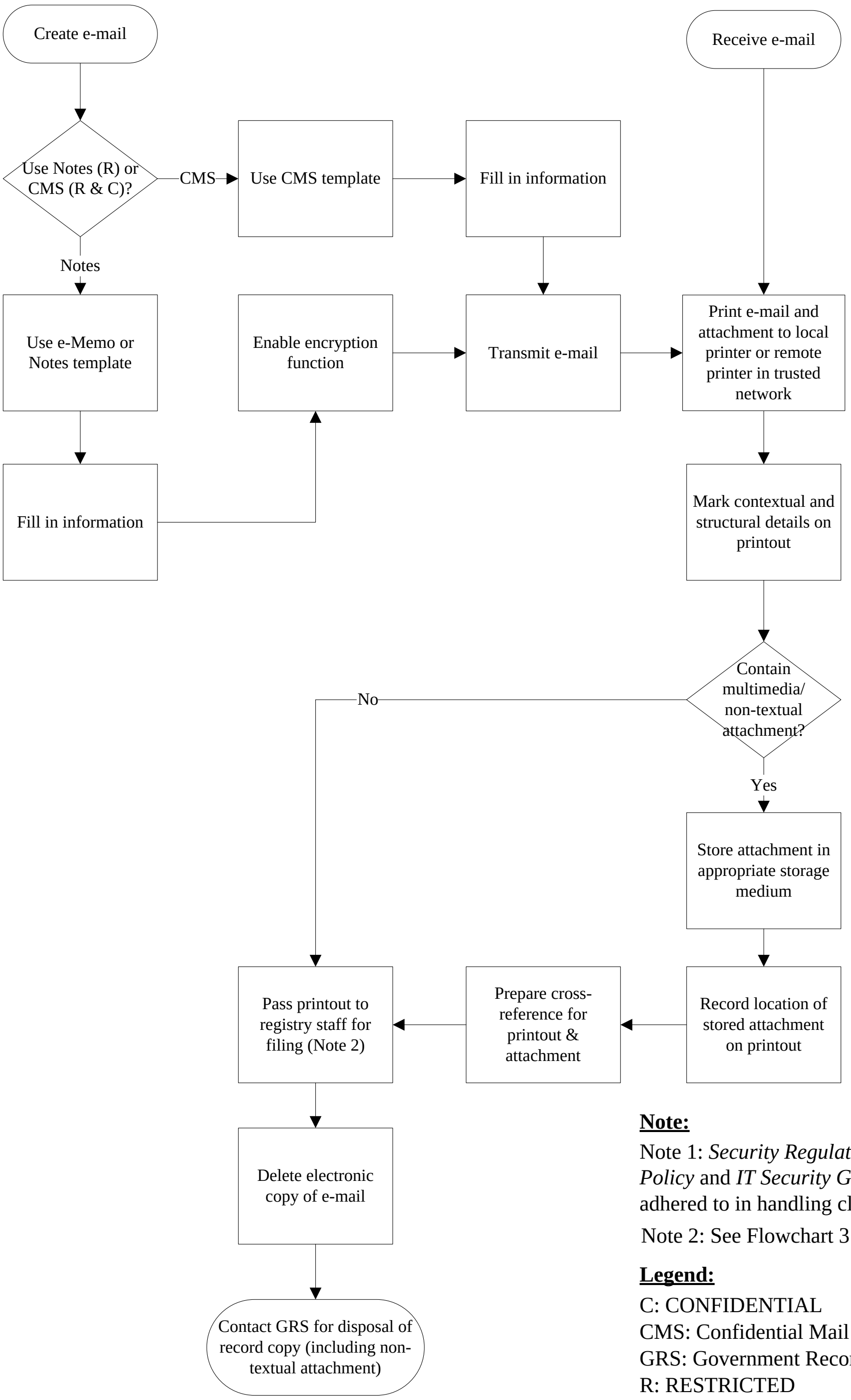
Note 1: See Flowchart 3 - "File E-mail Printout"

Legend:

GRS: Government Records Service

Flowchart 2

Create and Handle RESTRICTED and CONFIDENTIAL E-mail (Note 1)



Create e-mail
Use Notes (R) or CMS (R & C)?
CMS
Use CMS template
Fill in information
Notes
Use e-Memo or Notes template
Fill in information
Enable encryption function
Transmit e-mail
Receive e-mail
Print e-mail and attachment to local printer or remote printer in trusted network
Mark contextual and structural details on printout
Contain multimedia/ non-textual attachment?
No
Yes
Store attachment in appropriate storage medium
Record location of stored attachment on printout
Prepare cross-reference for printout & attachment
Pass printout to registry staff for filing (Note 2)
Delete electronic copy of e-mail
Contact GRS for disposal of record copy (including non-textual attachment)

Note:

Note 1: *Security Regulations, Baseline IT Security Policy* and *IT Security Guidelines* should be strictly adhered to in handling classified e-mail records

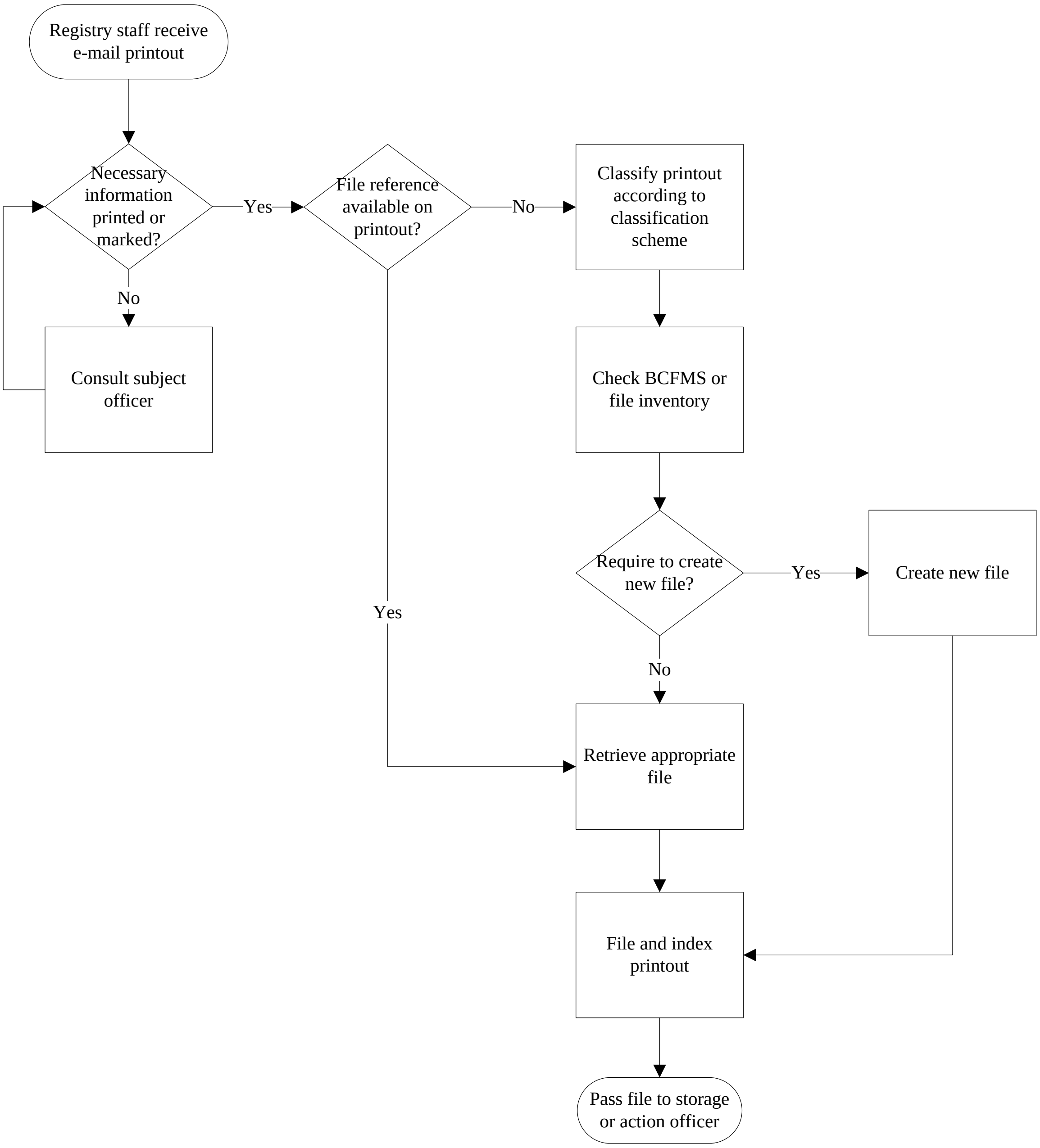
Note 2: See Flowchart 3 - "File E-mail Printout"

Legend:

C: CONFIDENTIAL
CMS: Confidential Mail Systems
GRS: Government Records Service
R: RESTRICTED

Flowchart 3

File E-mail Printout (Note 1)



Registry staff receive e-mail printout
Necessary information printed or marked?
Yes
No
Consult subject officer
File reference available on printout?
No
Yes
Classify printout according to classification scheme
Check BCFMS or file inventory
Require to create new file?
Yes
Create new file
No
Retrieve appropriate file
File and index printout
Pass file to storage or action officer

Note:

Note 1: *Security Regulations*, *Baseline IT Security Policy* and *IT Security Guidelines* should be strictly adhered to in handling classified e-mail records

Legend:

BCFMS: Bar-coding File Management System