Guideline on the Management of Electronic Messages

Government Records Service
Administration Wing
April 2024

Table of Contents

1. INTRODUCTION

Definitions

1.1 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.

"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.

"Social media" refers to forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos). Examples of social media platforms include Facebook, Instagram, YouTube, Weibo, etc. Please refer to Chapter 10 for more details.

"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 refer to Chapter 7 for more details.

Purpose and application of the Guideline

1.2 General Circular (GC) No. 3/2024 entitled "Management of Government Records" sets out (a) comprehensive guidelines on management of government records throughout their different stages of the life cycle; and (b) the updated list of mandatory records management requirements (MRs) for compliance of government officers.

1.3 Having regard to GC No. 3/2024, this Guideline gives guidance and instructions to help bureaux and departments (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.

1.4 In view of the increasing use of social media by B/Ds and Government officials in recent years, **Chapter 10 on "Management of social media records"** is added to this Guideline to provide further guidance to facilitate B/Ds to adopt the best practices in managing social media records. Same as other Government records, it is the responsibility of B/Ds to ensure that their social media records are properly managed in accordance with the prevailing records management principles and MRs.

1.5 This Guideline is intended for Departmental Records Managers (DRMs), records management staff (including registry staff), all users of electronic messaging (including e-mail) services, users of official social media accounts (including officers who are designated to oversee the management of social media records), 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.

1.6 The use of an ERKS for the management of records has been put in place in some B/Ds. As stipulated in GC No. 3/2024, B/Ds should capture electronic message records directly to an ERKS once implemented. Unless agreed by the Government Records Service (GRS) to dispense with the "print-and-file" practice after satisfying certain circumstances[1], all electronic message records should also be "printed-and-filed". This Guideline provides, among other guidance, standardised procedures for the "print-and-file" practice to ensure that the required information of an electronic message record will be adequately and effectively captured in a paper-based recordkeeping system.

1.7 Enquiries on this Guideline should be addressed to Senior Executive Officer (Record Systems Development)1 of GRS at 3468 6385.

[1] B/Ds which have implemented an ERKS should conduct a compliance assessment in accordance with the "Manual on Evaluation of an Electronic Recordkeeping System" and seek GRS' agreement to dispense with the print-and-file practice.

2. IDENTIFICATION OF ELECTRONIC MESSAGE RECORDS

Electronic messages as records

2.1 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[2]. Electronic message records include e-mail records and other electronic message records created in short message service (SMS), other instant messaging services (e.g. WhatsApp, WeChat, the instant messaging function of the Government's new e-mail system namely the Centrally Managed Messaging Platform (CMMP), etc.), and soical media platforms (e.g. Facebook, Instagram and YouTube). The prevailing records management principles and MRs as set out in GC No. 3/2024 are also applicable to the management of electronic message records.

2.2 To ensure that these electronic message records (including but not limited to e-mail records) are timely, accurately and adequately documented and are readily retrievable and usable as and when required, same as records in other forms, under normal circumstances, they should be captured in a departmental recordkeeping system (e.g. paper-based recordkeeping system or ERKS) within 30 days upon creation/receipt and under exceptional circumstances, records could be captured within three months.

Rules for identification

2.3 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.

2.4 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.

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

---

[2] 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).

Features of a complete electronic message record

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

2.7 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.

2.8 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

2.9 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.

3. FILING[3] OF E-MAIL RECORDS

3.1 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.

The filing responsibility

3.2 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

3.3 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

3.4 ERKS offers an effective and long-term solution to the management of electronic records in a hybrid records management environment. To enhance efficiency in preserving and managing government records, the Government has committed in the Policy Address Supplement published in October 2019 that all B/Ds should have rolled-out the use of ERKS by end-2025. Once implemented, B/Ds should capture e-mail records directly to an ERKS.

[3] 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.

Print-and-file

3.5 Unless agreed by GRS to dispense with the "print-and-file" practice, 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

3.6 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.

3.7 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 2.9 above).

3.8 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

[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).

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

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

3.10 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.

4. Filing OF ELECTRONIC MESSAGE RECORDS OTHER THAN E-MAIL RECORDS

4.1 The principles, guidelines and procedures given in Chapter 3 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. 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 2.9 above.

4.2 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 Chapter 7 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.

4.3 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 4.2 above for options to document the details of the discussion where an electronic message cannot be directly printed out or captured into a departmental recordkeeping system).

[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.

5. APPROPRIATE USE OF THE GOVERNMENT MESSAGING SYSTEM

5.1 The Government messaging system is installed primarily for official business communication. Lotus Notes, as part of 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). The Government is also rolling out CMMP to all B/Ds to replace Lotus Notes. CMMP is capable of sending and receiving e-mail and instant message.

5.2 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.

5.3 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

5.4 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

5.5 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.

5.6 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

5.7 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

5.8 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.

5.9 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

5.10 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

5.11 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

5.12 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.

5.13 Officers should not put the text all in capital letters as it will make the text

[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".

difficult to read. Moreover, uppercase text is often interpreted as having extra emphasis.

5.14 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.

5.15 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 2.9 above.

6. INFORMATION SECURITY IN RELATION TO THE GOVERNMENT MESSAGING SYSTEM

Responsibilities of B/Ds

6.1 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

6.2 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.

7. USE OF THIRD-PARTY MESSAGING SERVICES

7.1 With the wider rollout of CMMP in the Government, B/Ds should consider using the instant messaging service of CMMP for conducting their official businesses. However, B/Ds may, in consideration of their business, operational and records management needs, adopt third-party messaging services (e.g. WhatsApp, WeChat, Facebook, etc.) as well. 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 in accordance with their departmental records management policy and business rules for creation and collection of records. As mentioned in paragraph 2.1 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

7.2 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 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 5.8 and 6.2 above.

Creation of electronic message records

7.3 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.

8. DISPOSAL[8] OF ELECTRONIC MESSAGE RECORDS

Destruction of electronic message records

8.1 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 MRs as stipulated in GC No. 3/2024, 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 electronic message records.

Deletion of the electronic copy after filing

8.2 In general, after the electronic message record has been captured by the "print-and file" approach into a paper recordkeeping system or direct capturing into an ERKS, 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 8.4 below.

Destruction of non-records

8.3 Non-records such as the duplicate electronic version of electronic message records as mentioned in paragraph 8.2 above, convenience or reference copies of electronic message records and personal messages can be disposed of without separate agreement of the GRS Director.

Regular housekeeping

8.4 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

8.5 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

[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.

Public Records Office of GRS for details on transfer of such records with archival value to GRS.

9. MANAGEMENT OF CLASSIFIED E-MAIL RECORDS

Transmission of classified e-mail

9.1 Officers should use designated official e-mail tools, viz. CMMP, Confidential Messaging Applications (CMSG) with Lotus Notes, or their approved mobile versions to transmit classified electronic messages up to CONFIDENTIAL level.

9.2 Before transmitting confidential e-mails, officers must be equipped with the necessary facilities. In addition, officers should make sure that the recipient(s) are registered confidential mail users and the "Subject" and "File Reference" fields of the message to be transmitted do not contain classified information.

Printing and handling of RESTRICTED and CONFIDENTIAL e-mail records

9.3 In addition to the procedures given in paragraphs 3.5 - 3.10 above 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.

9.4 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.

9.5 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

9.6 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.

9.7 B/Ds should comply with the MRs as stipulated in GC No. 3/2024, 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. Chapter 8 of this Guideline also apply to the disposal of classified e-mail.

Related regulations and guidelines

9.8 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 are available on ITG InfoStation (https://itginfo.ccgo.hksarg).

10. MANAGEMENT OF SOCIAL MEDIA RECORDS

Background

10.1 With the advancement of technology and the flourishing of social media platforms in recent years, there have been a rapidly increasing number of Government officials and B/Ds making use of social media to enhance their communication with the general public and to conduct business.

10.2 As stipulated in GC No. 3/2024, "Records, irrespective of its physical format or media, are valuable resources of the Government to support evidence-based decision making, meet operational and regulatory requirements and are essential for an open and accountable government." It is also elaborated in paragraph 2.1 above that "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." In this connection, the prevailing records management principles and MRs are also applicable to the management of social media records.

Developing business rules for records creation and collection[10]

What records to be captured

10.3 In determining whether a social media content should be considered as record, B/Ds are recommended to apply the following questions –

a. Is the information only available on the social media site and related to service delivery?

b. Does it contain evidence of B/D's policies, business, or mission?

c. Is the content related to public consultation exercises?

d. Is the content providing formal advice or guidance (e.g. response to a query)?

e. Does the content trigger an internal process (e.g. request for information, complaint)?

f. Is the information required to meet B/D's specific operational needs?

[10] B/Ds are recommended to make reference to the Guidelines on Creation and Collection of Records (GCCR) to determine what social media records to be captured. (GCCR is available on CCGO at http://grs.host.ccgo.hksarg/cgp_guidelines.html or on GRS' website at https://www.grs.gov.hk/en/hksar_government_administrative_guidelines_on_record_management.html)

If the answers to any of the above questions are yes, it is likely that the content should be regarded as record.

10.4 B/Ds should apply the above questions as far as practicable to ensure that complete and adequate records have been captured. In this connection, B/Ds are recommended to review the content of the following official social media accounts and at the very least, to cover those messages posted by Government officials and B/Ds starting from the sixth term of the Government –

a. social media accounts that are set up under the posts of the senior officials or the names of B/Ds; and

b. social media accounts (including personal accounts in the names of the Principal Officials) that are managed by Government employees or contractors and the associated expenditure are funded by the Government. For instance, instead of creating official accounts, senior officials may prefer to use, or allow their offices to use, their existing personal accounts mainly for disseminating information related to/promoting the work of B/Ds upon taking up the appointment in the Government.

10.5 As for the personal accounts managed by the senior officials themselves, these accounts will generally also be perceived by the community as official accounts and its contents as official contents. B/Ds are therefore recommended to make reference to paragraphs 10.3 and 10.4 above in determining which contents in these accounts should be managed in accordance with Chapter 10 of this Guideline.

10.6 For messages posted by a third party onto a social media account, B/Ds should note that the ownership and copyright of these messages should rest with the person who creates the messages but not the social media account owner, and there could be copyright and privacy issues to capture these messages. In this connection, messages posted by a third party are normally not required to be captured. Nonetheless, B/Ds should consider and develop business rules as to whether some specific types of messages posted by a third party (e.g. an enquiry or a complaint that requires the concerned B/D's public response or separate follow-up actions) should also be captured; and follow the data protection principles in the Personal Data (Privacy) Ordinance in protecting the relevant personal data.

When to capture records

10.7 Records should be created/collected as soon as practicable in order to ensure that the reliability and completeness of records will not be adversely affected due to passage of time.

10.8 B/Ds are recommended to capture the final version directly from a social media platform after it is published. To ensure timely filing and make reference to the handling of records in other forms, social media records should also be captured in a departmental recordkeeping system within 30 days under normal circumstances. However, B/Ds should be aware that a social media provider might discontinue their service or delete information posted by its users at any time, and therefore should capture the records as soon as practicable. Please refer to paragraphs 10.13 and 10.14 below on the two approaches for capturing the content.

10.9 Or as an alternative, B/Ds may capture the content before it is published. This should be done in accordance with B/D's practices for other forms of media, for instance, the chain of emails which form part of the approval process for the content should be considered as records and captured in the departmental recordkeeping system.

Who to capture records

10.10 B/Ds should clearly specify their staff's roles and responsibilities of capturing records, and ensure that records are captured as a business routine. In this connection, B/Ds should designate officer(s) of appropriate rank to oversee the management of social media records. Capturing reliable, complete and adequate records is the designated officer(s)' duties and responsibilities, and they should consult their DRM or GRS for advice on records management issues.

10.11 If B/Ds have engaged external service providers to manage their social media accounts, they should determine whether the service providers would also provide capturing service. If yes, they should include in the terms of service agreement, among others, the requirements in capturing the social media content, such as what content to be captured, when to conduct capturing and the capturing method.

How to capture social media content

10.12 Once the social media content is identified as record by a B/D, it should be captured in the B/D's departmental recordkeeping system (e.g. paper-based recordkeeping system or ERKS). Before an ERKS is implemented in the B/D, social media records should be saved in a CD-ROM or DVD-ROM for filing in the paper-based recordkeeping system. Two approaches for capturing social media content directly from a social media platform after it is published are provided below –

(A) <u>Built-in function in the social media platform to export content</u>

10.13 Some major and most commonly used social media platforms (e.g. Facebook, Instagram and YouTube) offer built-in functions to facilitate users to

export content from their accounts. The export function is easy to use by following a procedural guide provided by the platform[11]. Options are provided to choose the desired data categories and date range for export. B/Ds can download and receive a ZIP file that contains the chosen file format including any requested images and videos. This approach provides flexibility for B/Ds to select what types of information to be exported at different intervals depending on their needs and then save the captured social media content to their ERKS[12]. In line with Government records in other forms (see paragraph 10.8 above), B/Ds are recommended to export the content on a monthly basis.

(B) Manual method to capture content

10.14 Under this approach, a copy of textual and pictorial social media content is saved either as print screen or Portable Document Format (PDF) and filed as soon as possible upon its transmission or receipt in accordance with the departmental records management policy and business rules for the creation and collection of records. Then the multimedia or other non-textual elements posted on social media platforms can be filed together in the ERKS[13].

Records Disposal

10.15 Same as Government records in other forms, B/Ds should establish disposal schedules for social media records to ensure systematic planning and orderly implementation of records disposal after records have been kept the right length of time to meet the purposes they are created and in compliance with legal or statutory requirements. Officers should consult DRM for advice on records disposal issues.

[11] The exported content can be chosen in machine readable HTML (HyperText Markup Language) or JSON (JavaScript Object Notation) format.

[12] Before an ERKS is implemented in the B/D (or its division/unit) concerned, the records have to be printed-and-filed to the paper recordkeeping system while the multimedia records should be saved in a CD-ROM or DVD-ROM for filing.

[13] Or in a CD-ROM/DVD-ROM as described in Footnote 12.

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:

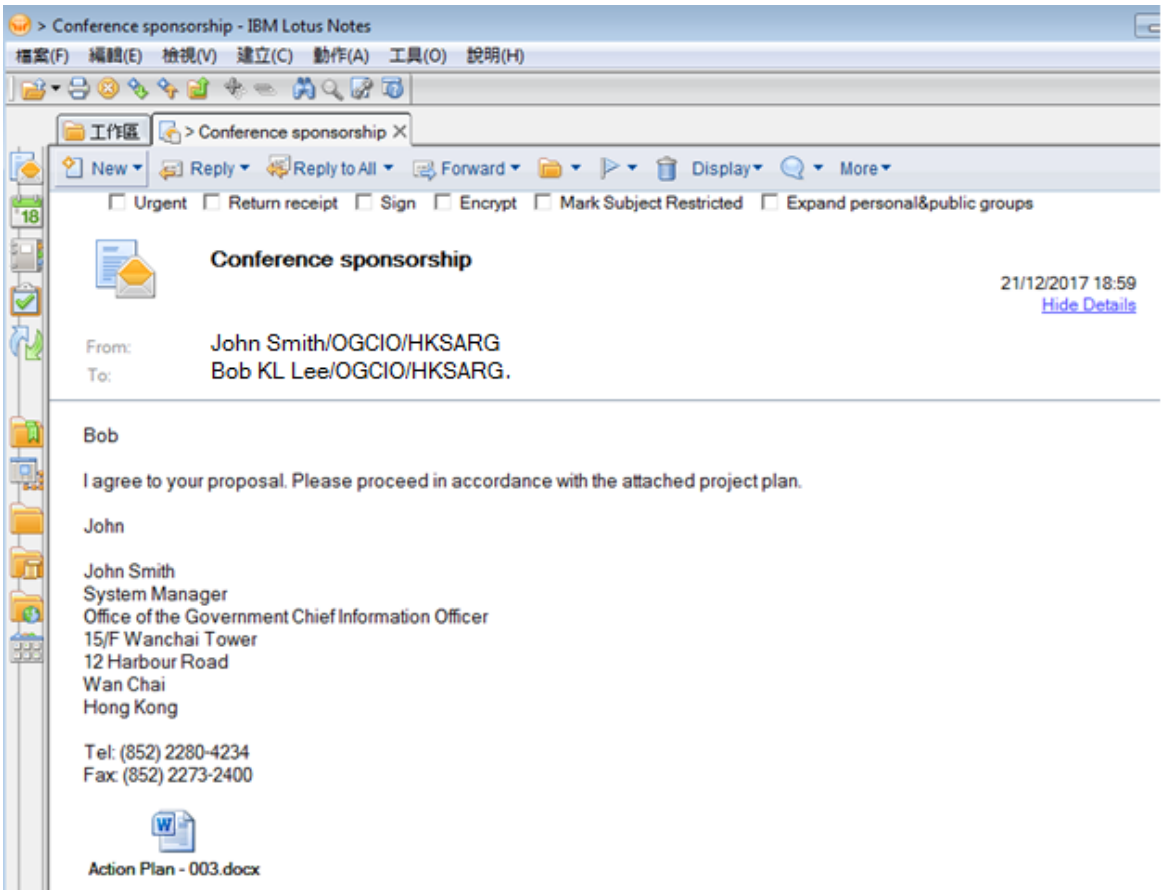
- Messages of personal nature
- Copies or extracts of documents that are published or downloaded and distributed for information or reference purposes
- Phone message slips
- Electronic copy of an e-mail record of which the record copy has been filed

Appendix B

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:



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).

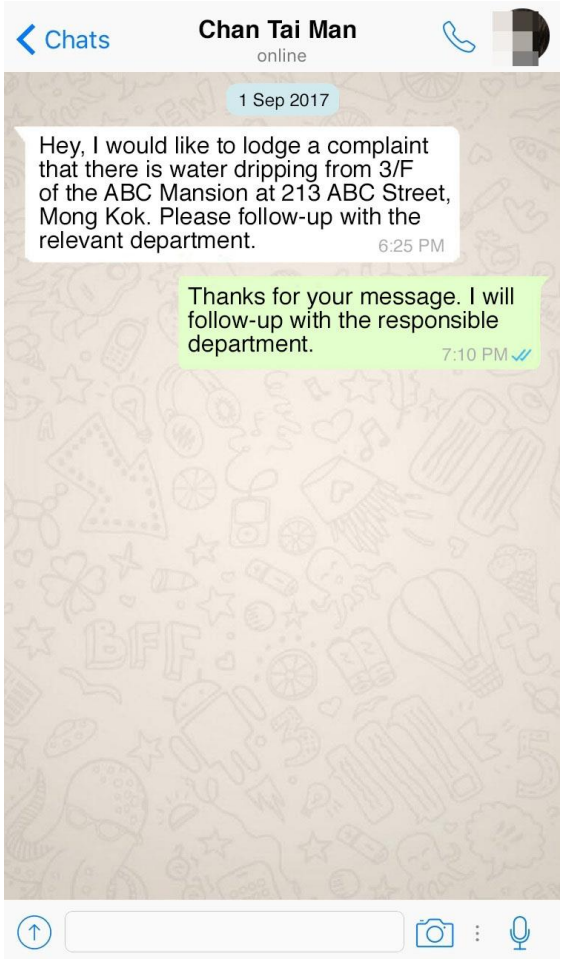
In the example above, the structure would comprise all of the elements that make up the documentary form of the e-mail message. These would include the header fields (not the information in the fields, only the headers themselves such as "to", "from", "subject", etc.), the length of the fields, their 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) An electronic message record other than e-mail record

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:



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).