



## **EFFICIENT AND ACCEPTABLE USE OF IT**

---

**February 2023**

**For review in: February 2025**



***To help the public service  
spend wisely***



# OAG POLICY: EFFICIENT AND ACCEPTABLE USE OF IT

---

- Purpose of the Policy ..... 1
- General principles in staff usage of information and technology (IT)..... 1
- OAG efficiency and collaboration practices ..... 2
- Basic security policies for staff..... 6
- Remote working protocols..... 8
- Responsible use of email ..... 10
- Responsible use of the internet..... 14
- Link with the provisions of the OAG Code of Conduct ..... 15
- Glossary ..... 16
- Appendix A: Approved software ..... 18
- Appendix B: Prescribed OAG storage ..... 18
- Appendix C: Password policy ..... 18




## PURPOSE OF THE POLICY


This Office of the Auditor General (OAG) issued this policy on the *Efficient and Acceptable Use of IT* to establish standards of use of IT made available to staff members. OAG provides IT to staff members to deliver, and help increase their efficiency at work. The policy also incorporates security practices adopted by OAG. The OAG has laid down guidelines in this policy in the context of its existing infrastructure, platform and services.


## GENERAL PRINCIPLES IN STAFF USAGE OF INFORMATION AND TECHNOLOGY (IT)

1. [OAG computers](#) owned by OAG, wherever used, are subject to these policies. In this policy, the term staff members include regular and temporary employees, as well as contracted staff if they are given access to the network or are issued OAG computers.
2. [OAG computers](#) issued to staff are intended for official use only, except for minimal personal use. The personal use of these resources is governed by the [OAG Code of Conduct](#) paragraph 48.
3. Staff should exercise the necessary diligence to safeguard [OAG computers](#) issued to them, particularly when they take them outside OAG premises.
4. Staff are expected to keep themselves reasonably aware of the risks to cybersecurity and avoid any suspicious item particularly from an external source. OAG's [IT Management](#) will provide ongoing updates and training to keep staff aware of cybersecurity risks and mitigations. Moreover, this policy includes some detailed guidelines related to the most common activities staff engage in like reading and sending out emails and browsing through the internet.
5. Staff should report any device malfunction or damage to [IT Management](#). IT Management shall ensure that the devices are promptly repaired or replaced. Staff will not be responsible for repairing or replacing OAG computers unless damage was caused due to negligence.
6. In exercising diligence, staff must consider the confidentiality of the digital information stored in [OAG computers](#).
7. Besides security awareness outlined above, staff are expected to observe office practices that advance efficiency and collaboration within the OAG, its clients and stakeholders. Office operations are highly-dependent on relevant

The legends below are used in this document, and clicking on the hyperlink will also take you there, or open the external document:

 Reference to a section or portion in this document

 Indicates an entry in the glossary for the meaning of the term

 Reference to a separate document

information that is available and up-to-date; [OAG efficiency and collaboration practices](#) (see the section below) support these objectives. Staff are also required to observe the OAG's [Social Media Policy](#), which extends to the personal use of social media on personal and OAG computers.

8. OAG will update staff on an ongoing basis on available technology and their capability to enhance effectiveness and efficiency in service delivery and corporate activities. OAG encourages staff to continually find ways that make our work more efficient while balanced with the security policies. Any such innovation should be approved by management before implementation, particularly if it is significant. Staff should consult with [IT management](#) on whether an innovation is significant.
9. Likewise, [IT management](#) will update staff and other stakeholders about cyber threats (including threats introduced by existing and new devices or software). [IT management](#) will issue alerts to highlight current events in cyber security. OAG will also issue or update its policies and procedures. Staff should take these updates into account in using OAG computers.
10. Staff must keep passwords safe and never share these in connection with network access and applications OAG uses with any other person, including co-workers. OAG will maintain and enforce a [password policy](#) across all managed systems. Use of the [OAG network](#) and [OAG computers](#) to view, transmit or otherwise handle (copy, edit, etc.) [inappropriate content](#) will be deemed gross misconduct and subject to the [OAG Code of Conduct](#).

## OAG EFFICIENCY AND COLLABORATION PRACTICES

11. This section describes existing practices among OAG staff in using technology that promotes efficient and effective working and collaboration. OAG encourages staff to observe them in the daily course of OAG work. However, a separate section below outlines policies and guidelines on the [Responsible Use of Email](#).

## AUDIT MANAGEMENT SOFTWARE

12. OAG has been using the Caseware as its audit management software. Caseware is essential for every financial and performance audit assignment. Its features include audit programs, sign-offs, review process workflow, risk report, internal controls and reportable items.
13. OAG recently added the feature to make Caseware available to OAG users of Citrix, while working remotely ([see below on how to access this](#)).
14. OAG allocates one Caseware licence for each staff member that is loaded on one [OAG computer](#) only. In cases where staff members choose to maintain a second [OAG computer](#) in line with



[OAG Flexible Remote Working Policy](#), staff need to be aware of this arrangement and the availability of Caseware in the Citrix environment when working remotely.

15. Signed-out and checked-out files (Caseware) should be backed up (signed-in and checked-in) within a reasonable period not exceeding 48 hours. Staff members should keep the rest of the audit team informed if signing out or checking-out files.

#### L DRIVE

16. The L Drive is the OAG's network drive and is the primary storage for OAG's records. Staff are encouraged to store new data using the existing folder structure to allow for information retrieval whenever needed.
17. Staff may create subfolders within their client folders in the L Drive. If a new sub-folder is needed in other locations (outside of client folders), staff should request [IT management](#) to create the sub-folder.
18. All official records must be stored on the L Drive, particularly corporate records, client information (Caseware files) and audit documentation. For clarity, staff members working offline on specific documents should:
  - a. transfer all of these official records from their local drives (C drives) to the L drive within a reasonable period not exceeding 48 hours.
  - b. be responsible for communicating with relevant team members that they are using files offline, and ensure that no version issues would occur (e.g., changes made offline by two team members cancel out each other, resulting to lost work).

#### SHAREFILE

19. Staff should use ShareFile site ([govky.sharefile.com](http://govky.sharefile.com)) of the Cayman Islands Government (CIG) when clients transfer information for financial and performance audits, special investigations and any other approved OAG assignments. Staff working on audits should create folders and manage access rights of clients and other users (grant, restrict or modify).

#### CALENDARS (OUTLOOK)

20. Calendars hold important information relevant to the rest of the office. Staff should update individual calendars on Outlook by:

- a. Sharing calendars to all OAG staff, including details. Those details could help colleagues in planning meetings and events. [Click here for Microsoft.com instructions on how to share calendars.](#)
- b. Activating the out-of-office notification for any period of absence.
- c. Noting days off (leave or TOIL), working from home and at clients' premises, as OAG will use it as a staff locator hub. (Refer to the [OAG Flexible Remote Working Policy](#))
- d. Sending invites for meetings with Zoom link and/or meeting room (a single invite can be sent with a room reservation and a Zoom link). OAG users may access Government Administrative Building (GAB) meeting room calendar when creating meeting invites.
- e. Before sending invites, staff should check the availability of those involved in their meeting or event. This can be done by:
  - i. Viewing multiple calendars side-by-side
  - ii. Viewing the Scheduling Assistant.
- f. Responding (accept or decline) to meeting invites like any other official email.

## ZOOM

21. Virtual communication (VC) is vital to the efficient and effective conduct of OAG business. The OAG platform supports Zoom, Microsoft Teams, Google Meet, Gotomeeting and Webex. OAG staff can participate in a virtual meeting or event using any of the above VC software but should be aware that anything beyond this listing should be vetted for cyber-safety before use. CIG provides Zoom corporate subscription to all staff. Therefore, by default, staff should use Zoom in organising meetings or events. Staff should note the following features available to them under this subscription:

- a. Organising and hosting virtual meetings.
- b. Virtually attending webinars or meetings organised by others in Zoom.
- c. Chatting with Zoom users (Zoom automatically authenticates CIG users under the subscription programme, and Zoom maintains a directory of these users. By typing their names on the chat, users can quickly initiate a chat with an authenticated user).

- d. Recordings of meetings or events are mostly not needed. But when needed, zoom meetings or webinars can be recorded by the meeting host. In such situations, the host must notify all attendees that a recording will be made well in advance. Zoom will obtain participant consent digitally.
- e. Zoom can be installed on a device app (Android or iOS) and facilitates [remote working](#), including secured chatting. The mobile version will mirror the activities on the desktop app when signed in with the same username and password.
- f. Chat and video from this subscription are stored on-premise (not on an external cloud) and do not add to the cyber security risk.

---

#### ELECTRONIC TIMESHEETS AND LEAVE SOFTWARE

- 22. Staff enter their timesheets currently on TRS. However, OAG will adopt a new electronic timesheet system shortly after the issuance of this policy. Staff should enter their timesheets using the software prescribed by OAG management. It is good practice that staff enter timesheets at the end of each working day. Staff should enter timesheets for each calendar week by the following Monday's close of business. Additionally, if any given month's last day falls on a weekday, staff should complete timesheets up to the month-end by close of the first business day of the following month. OAG's monthly financial close includes billing for the time charged to all audits being worked on which depends on complete and accurate timesheets for the whole month.
- 23. OAG is currently using MyVista as its leave tracking software. Staff should use this software to put in leave requests and track remaining entitlements (balances) to all types of leave available to staff. Ideally, staff should discuss their leave plans prior to submitting a request in the leave software. Once a request is made by staff, the respective manager reviews and approves it and is second-approved by a senior manager.

---

#### OTHERS

- 24. IRIS or Oracle E-Business Suite is the CIG's main system for financial accounting and reporting, purchasing and payments, and revenues and receivables among others. In the IT industry, IRIS is classified as an enterprise resource planning (ERP) software. Two types of accesses are granted to OAG staff depending on roles:
  - a. Audit access – view only (on transaction or balance inquiry) granted for all entities

- b. Operations user access – granted for the two OAG entities (10 and 52) to employees with corporate finance or HR roles.<sup>1</sup>

25. Staff should use the updates including but not limited to the following sources as relevant to their work requirements:

- a. The Hub, CIG’s intranet system
- b. “News Today” emails and other corporate and practice matters broadcasted via email to staff.
- c. OAG subscribes to Caymancompass.com as we expect staff to follow the news, particularly those that OAG circulates daily.

26. More and more, our work could be done digitally (on-screen) without printing. Therefore, staff should consider avoiding printing, but each individual should feel free to print documents at their discretion.

#### **BASIC SECURITY POLICIES FOR STAFF**

27. Password control is in effect for all [OAG computers](#). This currently follows the processes in place for CIG. All OAG staff should safeguard their password by observing sensible practices, including:

- a. Never share passwords with anyone, including fellow staff members.
- b. Avoid writing down their passwords.
- c. Avoiding weak passwords, including short passwords and common words or information (like birthday/year, “Cayman”, “Password”).
- d. Avoid using passwords already used for other accounts, particularly those used for personal accounts like email, shopping, etc. A compromise in those external sites could also render staff’s work account vulnerable.

28. Accounts (username and password) and computers are controlled by the Computer Services Department as they are how legitimate users access information and other technology resources.

---

<sup>1</sup> IRIS terminology for a separating financial reporting organisation is ‘entity’. OAG has two reporting ‘entities’ whose codes are 10 (Entity) and 52 (Executive).

Malicious actors could use these legitimate routes to gain access to steal, destroy or otherwise alter information. Standard network policies are in place (CIG-wide) to manage this risk. One factor that heightens this risk is when accounts or devices are inactive for long periods. When staff experience access denials arising from these security (network) policies, they should immediately reach out to CSD Helpdesk staff, who can restore access to accounts or devices, either via 244-2000 or by emailing [cshelpdesk@gov.ky](mailto:cshelpdesk@gov.ky). Instances in which accounts or devices are locked out include the following:

- a. A user account will be disabled if it has not been on the [OAG network](#) for 30 days or shorter if directed by the Auditor General.
  - b. A device will be disabled if it has not been on the [OAG network](#) for 30 days.
29. Direct connection (e.g., via Bluetooth and USB cables) between [OAG computers](#) and personal devices is allowed for charging personal devices. However, data transfer between an OAG computer and any removable media (e.g., USB drive) is not allowed. This practice increases the risk of malicious software infecting the OAG computer and OAG network. It also exposes data stored on removable media to being lost (and disclosed) accidentally or maliciously. OAG staff should request the information be placed on ShareFile (see section above) from external parties (like clients) rather than requesting or accepting on a removable media. If this is not possible, [IT Management](#) needs to approve the use of removable media. The IT Management will ensure that security protocols are observed to prevent the introduction of unwanted software.
30. Moving or keeping work-related information on storage outside of the OAG network and [OAG computers](#) is strictly prohibited as they are not [prescribed secured storage](#). For example, the following cannot hold work-related information:
- a. Personal devices, including laptops, tablets and phones.
  - b. Personal emails and cloud accounts.
31. Physical security will be observed by staff as follows:
- a. Observing OAG premises security protocols.
  - b. Use the OAG-issued device lock at all times (for both devices on-premise in OAG and remote working). Staff should consider that client workspaces are not familiar; the risks are generally higher.

- c. [Remote working](#) introduces other risks depending on the living arrangements of staff. Staff should be aware and sensible to ensure secure remote working and follow OAG's [Remote Working Protocols](#).
32. Through staff updates, staff will become more cyber-aware, enabling them to identify unexpected behaviour of systems and devices. OAG staff should report any suspicious behaviour of devices to the IT Management or [Security Operations Centre \(SOC\)](#) at the first chance available; in their absence, any member of OAG management. In addition, OAG staff should also report the following:
  - a. Possible breach of security, physical or logical controls
  - b. Unauthorised access
  - c. Disclosure of OAG or client data (data protection), which OAG staff should also report to the OAG's Data Protection Officer. (This includes accidental disclosure e.g., if emailed to someone unintended.)
33. Only software included in the [Approved Software List](#) can be installed on [OAG computers](#). OAG management will consider and approve adding software to this list. Staff should submit a request to Deputy Auditor General (Corporate and International) for software, providing information about the application and the business reason for installing it.

## REMOTE WORKING PROTOCOLS

34. [Remote working](#) means performing duties in a location other than within OAG premises. This includes working at clients' premises, at home or while travelling for work. The risks are generally in the two aspects of the physical environment and remote digital connection. In all instances, remote working introduces a certain level of additional security and efficiency risks. For example, personal wi-fi security at home can vary depending on the settings. Staff members should be aware of these risks, and where necessary, consult internally or research (using reliable sources) on how to increase security while working remotely.
35. Staff remotely working in the Government Administration Building (GAB) can connect their OAG computers to the CIG network. (Tip: take your cables with you for fieldwork to ensure you have one to use). However, staff should take steps to maintain security, such as:
  - a. Before plugging into the network, inquire from client personnel where you should connect rather than looking for the connections yourself. This simple, sensible step

guards against compromised ports. It is not a high-likelihood risk, but it can impact the device and data if it happens.

- b. Normal security awareness should be exercised at all times, particularly when handling sensitive information (e.g., payroll) during client visits that can be seen by people around.
  - c. When working in any client premises outside of the GAB, staff should use Citrix.
36. Staff may work remotely in other departments, statutory authorities and government companies' office (outside GAB) using CIG's Citrix Environment. CSD tailored the OAG Desktop in Citrix for our staff (which includes Caseware). Staff will also use the Citrix Environment when they are working from home. However, staff may experience performance issues. Performance issues refer to slower computer response speed, i.e. remote working with Citrix could be slower than working on-premise. These are usually hard to troubleshoot while working remotely; the internet connection (e.g., at home) plays a primary role in whether the speed is acceptable. Staff should seek help from CSD Helpdesk, including their out-of-hours number (925-0394) if needed.
37. [Remote working](#) generally heightens security risks from the internet connection and the working environment. When connecting [OAG computers](#) to external routers, staff should be aware of how secure their connection is. Examples where connection risks are higher than what is acceptable include but are not limited to:
  - a. Router not password protected, including home wi-fi.
  - b. Your device's security software (Microsoft Defender) highlights a specific risk.
38. If warranted by the situation, staff should then take sensible steps to ensure that their connection is secure enough, including but not limited to the following:
  - a. As a precaution, always make the computer hidden from other users in that network.
  - b. Delay any non-urgent work while working outside of a network with an acceptable security level.
  - c. Work entirely within the Citrix environment.
  - d. Many routers are password protected (e.g., at home), providing a layer of protection. However, OAG staff should consider password strength (you may use our [password policy](#) as a guide if you want to strengthen your home wi-fi password).

- e. There are also instances when the home router's default password was not changed after purchase. This risk needs immediate resolution.
  - f. The [remote working](#) computer is routinely re-attached to the on-premise [OAG network](#) (up to the point of checking for security patches and updates). This will push security and other updates to [OAG computers](#).
39. OAG and [SOC](#) will monitor activities during [remote working](#) to identify unusual patterns or other activities that may appear suspicious as a cyber prevention process.

#### RESPONSIBLE USE OF EMAIL

40. Emails should be written clearly and while observing the OAG values bearing in mind that they will likely be permanent records and subject to laws. Emails are subject to the following laws and their related regulations and guidance, particularly in regards to their confidentiality, disclosure, retention, archiving and deletion:
- a. National Archives and Public Record Act – specifies a period of retention of records, and certain requirements at the time of disposing government records
  - b. Freedom of Information Act – encourages proactive and by-request release of government-related information
  - c. Data Protection Act (Note: OAG has a [Data Protection Policy](#)) – requires Cayman Islands public sector and private organisations to comply with standards that advance the rights of individuals with regards to sensitive and personally-identifiable information relating to them
41. Emails are a significant area of cybersecurity threat. In keeping with the separation of work and personal devices and accounts, in all cases, staff should not use personal emails for any work-related purposes.
42. The everyday email addresses used by staff end in [[@oag.gov.ky](#)]. Staff should likewise be aware that emails sent to their [[@gov.ky](#)] email addresses will successfully reach the same email box. [IT Management](#) ensures that email accounts are created:
- a. Upon hiring a new employee, including temporary staff and interns.
  - b. As functional/shared email accounts and shall be subject to specific requirements.
43. [IT Management](#) shall make sure that email accounts are deactivated promptly:



- a. Upon departure of an employee, including temporary staff and interns.
- b. Management decides to discontinue a shared email address.

---

#### PREVENTING CYBERSECURITY EVENTS FROM INBOUND EMAILS

44. Inbound emails (emails you receive) pose a wide range of threats to individual and shared digital workspace. The OAG will periodically remind and provide refresher training about cybersecurity risks, including perpetrators' use of email.
45. Using OAG email addresses to subscribe to newsletters carries additional risk each time it is used to sign-up. This is related to the possibility that a cybercriminal could steal (or other malicious transfer) email addresses, which will translate to future attacks targeted at compromised addresses. OAG staff should observe the following guidelines:
- a. Business use of the OAG email address is allowed, but personal use to sign-up should be minimised. OAG staff should not use OAG email addresses for e-commerce, sellers and other marketing websites. This combination of practices will limit the likelihood of spam and other cyber risks.
  - b. OAG staff may use their OAG email addresses for personal use in dealing with CIG entities and their professional institutes, as this practice does not add any risks.
46. Attachments and hyperlinks are common vulnerabilities to allow attacks into the network. OAG staff should be mindful of the risks and take utmost care to prevent any cybersecurity events. These prevention steps include but are not limited to:
- a. Make sure that the underlying email addresses are legitimate. Users should be aware that there are ways to spoof the written names of senders when the actual email address could be different. When a recipient drills down on the sender's email, it will become apparent that it is spoofed. Malicious actors send emails with spellings and syntax designed to confuse email recipients, by making emails look legitimate.
  - b. Not opening email attachments from unknown sources or attachments from unknown sources that are suspicious or unusual. Picking up the phone to verify with the sender that the email is from them is a simple way of addressing this risk.
  - c. Heed the warnings embedded by our email system that inbound emails are coming from outside the network and exercise the appropriate level of caution.

---

## USING INBOUND AND OUTBOUND EMAILS

47. Upon receipt of inbound emails, individual staff members are responsible for judging emails' urgency and to immediately action genuinely urgent emails. Staff should acknowledge inbound emails even when final action or resolution is not imminent.
48. Sending emails is generally appropriate when sending a formal notification or message, particularly to clients, but also for internal OAG purposes. Other ways staff could use Outlook for efficiency and documentary purposes include the following:
- a. Voting buttons enable recipients to respond to specific questions and the sender to get the results tabulated in Outlook. The respondents need to use the original email to respond.
  - b. Creating a record of discussions (see subsection b of the next paragraph).
  - c. In rare circumstances, staff may require time stamps for receiving and read receipts and should be activated only for only specific messages.
49. However, the following and similar practices are discouraged:
- a. Transferring large and numerous files. Email attachments support the message within the email body, but staff should not use emails to bulk-transfer files. Use ShareFile if this is the case.
  - b. Back-and-forth emails that mimic chats or phone calls might merit an actual face-to-face discussion, chat or phone call. An app called [MiCollab](#) (Android and iOS) is available to staff. This mobile app taps into our office phone lines and does not use our personal mobile minutes. Additionally, Zoom Chat is available. After discussing, OAG staff could send an email to create a record of the conversation, particularly if any key matters need to be evidenced (as in an audit).
50. In crafting emails, including replies, OAG staff are expected to observe the following principles:
- a. In keeping with our core values of professionalism and respect, staff should communicate using email while ensuring utmost courtesy.
  - b. Email use is forbidden for any unlawful or immoral purpose or any activity dealing with [inappropriate content](#). This prohibition includes but is not limited to copyright infringement, obscenity, slander, fraud, computer tampering, etc.

---

## ORGANISING OAG EMAILS

51. Staff should periodically organise and manage emails according to existing guidance issued to the civil service (see succeeding two paragraphs). In doing so, staff help ensure compliance with related laws and regulations (see list of laws above).
52. The Cayman Islands National Archives (CINA) have issued guidelines to the civil service in determining what messages constitute official records. OAG staff emails should be kept (and not immediately discarded) according to the record retention policy. According to CINA's Guideline 8 – Managing Electronic Records, staff should ask these questions when deciding whether an email is an official record. When the answer to any one of them is 'yes', the record should be treated as an official record and retained according to the documentation policies of OAG:
- a. Does it approve or authorise actions?
  - b. Is it a formal communication between staff relating to work?
  - c. Does it signify a policy change or development?
  - d. Does it commit my organisation to an arrangement or to a business deal? (OAG note: Copies of executed contracts may be sent as email attachments but good practice precludes entering into a contract by exchanging emails with a counterparty.)
  - e. Does it contain advice, provide guidance or constitute formal communications with people inside or outside the organisation?
  - f. Am I required to act upon it?
  - g. Is it external correspondence I have received relating to work?
  - h. Is it something that I have sent for a business purpose?
  - i. Is it something I have used at work to make a decision?
  - j. If I left this job tomorrow, would my successor need the information in this message to continue with this matter?
  - k. Is the matter to which the message relates one which may be reviewed or audited later?
53. In Guideline 8 above, CINA adds specific guidelines when deleting emails. Staff should observe this guidance when cleaning up their mailboxes:

- a. Many emails can be deleted because they are copies, temporary or ephemeral. These should be disposed of as soon as possible. No further authorisation by means of disposal schedules is required. Examples of emails that fit within this category are:
  - Copies for information only.
  - Copies of the same email in different folders.
  - Memos, notices, announcements to all staff, including CS Messages.
  - Drafts which you have read.
  - Personal emails.
  - Junk mail or SPAM.
  - Out of office and other automatic responses.
- b. Official emails should be deleted from your inbox when they are no longer needed as records, because you are certain that they have been printed/saved and filed in the official filing system. (OAG note: Our team prefers capturing email copies in PDF and stored in the appropriate network location, e.g. an audit file. In addition, staff should delete these items from their 'deleted items' as well).
- c. Use email folders to manage emails you keep electronically for reference purposes. This should be structured to match your file plan.

## RESPONSIBLE USE OF THE INTERNET

54. The OAG provides internet access through the [OAG network](#) and the secured OAG wi-fi. Internet through the [OAG network](#) is provided primarily for business purposes. OAG staff and guests are free to use the OAG wi-fi for personal use.
55. Staff and guests should not use the OAG wi-fi for illegal or immoral purposes or otherwise dealing with [inappropriate content](#). Specifically, OAG prohibits the use of the internet (In both [OAG network](#) and OAG wi-fi):
  - a. To access sites that are offensive to a person's gender, sexuality, religion, nationality or politics.
  - b. Other sites that can adversely impact staff productivity, such as gaming.
  - c. Downloading from unsafe or non-reputable websites (particularly when there are warnings on sites one is attempting to visit).
  - d. To download executable files, pirated music, movies and software.

56. Hyperlinks sent through emails are a common tactic of cyber perpetrators to lure potential victims to malicious sites or download malicious software. OAG staff should be aware of the link between the responsible use of emails and the responsible use of the internet to prevent cybersecurity events.
57. OAG reserves the right to monitor internet usage over the [OAG network](#). Currently, the CIG's [SOC](#) monitors the [OAG network](#) following CIG security protocols. Keeping our devices and network secure necessitates the responsible use of the internet using the OAG network and the OAG wi-fi.
58. The [SOC](#) may email [IT Management](#) and/or the staff member concerned when cyber risk monitoring systems alert them about sites staff visit that are potentially risky. Staff should promptly answer (with a copy to [IT Management](#)) any inquiries and cooperate with the [SOC](#) regarding activities on the internet that it may flag. A number of experiences by some OAG staff showed that websites flagged by [SOC](#) turned out harmless. The SOC follow their protocol in resolving these issues when they arise.
59. In addition to personal emails, chat applications on personal devices are used to discuss matters that could be OAG work-related. OAG staff should not use these channels for official communications or confidential matters, particularly social media platforms that are not end-to-end encrypted. For example, all OAG staff participate in a Whatsapp group mainly for social and non-sensitive information being broadcasted quickly to all staff, but not for anything sensitive, confidential or the like. This example presents a sensible rule of thumb on the limits of mixing work and messaging platforms.

#### LINK WITH THE PROVISIONS OF THE OAG CODE OF CONDUCT

60. The Code of Conduct provides a process for reporting and dealing with breaches of these policies, including whistleblowers.
61. The Office reserves the right to maintain activity logs, monitor and review activities and investigate (including asking for expert assistance) to enforce OAG policies.

## GLOSSARY

Citrix	<p>Citrix is the brand name of the remote access (virtual private network or VPN) used by the Cayman Islands Government (CIG) which is used by OAG staff.</p> <p>By usage in the workplace, this refers to the virtual desktop (non-physical) that staff gets access to when working remotely to obtain secure access to data and applications accessible when on-premise.</p>
IT Management	<p>Either or both of the: Deputy Auditor General Corporate and International and the Audit Manager – Quality Assurance and IT.</p>
Inappropriate content	<p>Downloaded files or internet copies (including emails and attachments) of any data or media that is generally offensive, immoral, illegal, or harmful to the security of the OAG network and devices, including but not limited to:</p> <ul style="list-style-type: none"> <li data-bbox="621 968 824 993">• Pornography</li> <li data-bbox="621 1041 781 1066">• Gambling</li> <li data-bbox="621 1115 1385 1178">• Sites where there is a risk of exposure to spam, phishing and malicious software</li> </ul>
MiCollab	<p>Software provided by Mitel, CIG’s landline handset vendor. It allows user to remotely use their office landlines (244 numbers) on their computers or landline and installed on computers and mobile devices</p>
OAG computers	<p>Any desktop or laptop computer, including Microsoft Surfaces or equivalents that OAG owns and assigned to individual staff. This excludes any mobile devices like phones or tablets that may be issued to staff.</p>
OAG network	<p>The OAG Platform, including any network, internet connection, and all end-points like individual OAG computers, printers and the like. It also encompasses any cloud storage which OAG maintains.</p>
Personal devices	<p>Any computer, tablet or smart phone that is owned by an employee or contractor, particularly if persons use them for OAG business or connects them to OAG wi-fi.</p>

Personally identifiable information	Or <i>personal data</i> under the <a href="#">Data Protection Act</a> , means data relating to a living individual who can be identified and includes data such as (a) the living individual’s location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the living individual; (b) an expression of opinion about the living individual; or (c) any indication of the intentions of the data controller or any other person in respect of the living individual.
Remote working	Performing work duties in locations other than OAG premises, particularly while using <a href="#">OAG computers</a> .
Sensitive personal information	Or <i>sensitive personal data</i> under the <a href="#">Data Protection Act</a> , are personal data consisting of: (a) the racial or ethnic origin of the data subject; (b) the political opinions of the data subject; (c) the data subject’s religious beliefs or other beliefs of a similar nature; (d) whether the data subject is a member of a trade union; (e) genetic data of the data subject; (f) the data subject’s physical or mental health or condition; (g) medical data; (h) the data subject’s sex life; (i) the data subject’s commission, or alleged commission, of an offence; or (j) any proceedings for any offence committed, or alleged to have been committed, by the data subject, the disposal of any such proceedings or any sentence of a court in the Islands or elsewhere.
Security Operations Centre (SOC)	A functional area within the Cybersecurity Unit of CIG that monitors and investigates potential breaches based on set parameters using automated monitoring tools.  The SOC also provides advice, training, awareness activities and issues CIG-wide alerts on cybersecurity matters.

## APPENDICES

---

### APPENDIX A: APPROVED SOFTWARE

1. Audit Management Software – both Caseware Working Papers and Caseware Audit Template
  - a. Add-in: Caseware Connector
2. Mindgenius (Mind Mapping software)
3. Caseware Analytics or IDEA
4. AuditSampler
5. Adobe Pro
6. KPMG's PDF Retention File Viewer
7. Zoom
  - a. Add-in for Outlook

### APPENDIX B: PRESCRIBED OAG STORAGE

The following are OAG-sanctioned digital spaces where OAG staff may store work information:

1. The L Drive
2. Extant U Drive
3. Hard drive of each [OAG Computer](#), subject to security and data management policies

### APPENDIX C: PASSWORD POLICY

1. OAG requires individual passwords for the following accounts:
  - a. Main network (AU) account (same username and password to be used for MyVista)
  - b. TRS account (also using AU for user name, but password could be different)
  - c. IRIS access (one account for either or both corporate OAG and Audit Access)



- d. Zoom
  - e. Cayman compass
  - f. TheHub.gov.ky
2. The following devices shall be subject to password protection governed by the policies:
    - a. [OAG Computers](#) issued to staff
    - b. Office-issued devices where emails and other “prescribed applications” are authorised to be used.
    - c. Personally-owned devices where emails and other “prescribed applications” are authorised to be used.
  3. The general password strength standards are as follows:
    - a. Minimum eight characters.
    - b. Must contain all these types: alpha and numeric only.
    - c. Passwords should be unique and not reused.
  4. The general password longevity is 90 days.
  5. Lock out is enforced after three failed attempts at authentication (i.e., entering username and password). Users need to contact CSD Helpdesk (244-2000 or after hours 925-0394) to lift the account lock. CSD will re-open the account once satisfied that the person requesting it is the account owner.