NICS Internal Audit Services

better insights, better outcomes

TO: COVID-19 HOCS Reference Group

FROM: Tracey McCavigan
Group Head of NICS Internal Audit Services

DATE: 07 December 2023

SUBJECT: NICS Mobile Device Fact Finding Investigation

Please find enclosed for your information and consideration the final report on the above mentioned investigation.

The Investigation Team would like to thank management and staff for their co-operation and assistance.

NICS Internal Audit Services

better insights, better outcomes

NICS Internal Audit Services

NICS Mobile Device Fact Finding Investigation

Date: 07 December 2023
CM Ref: FI1/23/1259756

TABLE OF CONTENTS

1. INTRODUCTION, SCOPE, BACKGROUND AND WORK UNDERTAKEN

1.1 Introduction

1.1.1 NICS Internal Audit Services were asked by the HOCS Reference Group to undertake a fact finding investigation across the NICS following a potential disclosure issue being identified in relation to the ongoing COVID-19 Public Inquiry.

1.1.2 Specifically, it was identified that a number of NICS issued mobile devices containing information that may be potentially relevant to the COVID-19 Public Inquiry (for example text messages and WhatsApp messages) had been erased/reset prior to being returned or on return, thus impacting the ability for full disclosure.

1.1.3 These concerns related to smartphones and tablets issued to NI Executive Ministers (including the First Minister (FM) and deputy First Minister (dFM)) and their associated Special Advisors (SpADs).

1.2 Scope

1.2.1 The agreed objectives for this investigation were:

- To physically locate and secure the relevant mobile devices;
- Establish what mobile device or relevant policies, procedures, guidance and processes were in place across the NICS at the time of the devices being returned;
- Establish what specific guidance or instructions have been issued relating to retention of information held on mobile devices for the Inquiry;
- Establish what steps (if any) were taken to identify and/or retain relevant information on the mobile devices; and
- Document the circumstances that led to a number of mobile devices being erased/reset prior to being returned or on return, including whether this was

in line with the relevant policies, procedures and guidance in place at that time.

1.3 Scope Limitations

1.3.1 If analysis of the mobile devices by an IT specialist is required in order to confirm the status of each device and to retrieve information where possible, this would be undertaken as a separate exercise.

1.4 Background Information

1.4.1 On the 12th May 2021, the Prime Minister announced that there would be a UK-wide COVID-19 Public Inquiry and on the 10th June 2021 the Director General, Propriety and Ethics from the Cabinet Office wrote to all Whitehall Permanent Secretaries notifying them that a statutory Inquiry into the COVID-19 pandemic would be taking place covering the period January 2020 to June 2022, potentially commencing in spring 2022. He asked that they take steps to assure themselves that they would be ready to meet obligations to provide relevant records, information and data to the Inquiry. This communication was also copied to the Head of the Civil Service (HOCS) who subsequently forwarded this correspondence to NICS Permanent Secretaries on the 14th June 2021.

1.4.2 On 16th September 2021 and 28th October 2022 HOCS wrote to all NICS Permanent Secretaries reiterating the need to take steps to assure themselves that Departments and ALBs would be ready to meet their obligations to provide relevant records, information and data to the Inquiry. HOCs also wrote to all NICS Permanent Secretaries on 28th July 2022, however this correspondence primarily related to the matter of whether departments should consider applying for designation as Core Participant (CP) status for Module 1 of the Inquiry.

1.4.3 Within the September 2021 HOCS correspondence specific guidance was attached; DSO preliminary guidance in advance of any COVID-19 Public Inquiry. Section 4 stated "*Although the Terms of Reference are yet to be published, it is very likely that all documents pertaining to COVID-19 may be relevant to the Inquiry. This will include:*

- *Hardcopy documents (e.g. draft minutes, notebooks, internal forms, handwritten notes, diaries); and*
- *Electronic documents (e.g. email and other electronic communications such as text messages, WhatsApp messages and voicemail, word-processed documents and databases, and documents stored on portable devices such as memory sticks and mobile phones)*".

The document also states within this section that "*If documents that are relevant are destroyed, the Inquiry can publicly criticise the department and may draw inferences from the fact that the Department did not take appropriate steps to preserve relevant documents are the earliest opportunity*".

1.4.4 A NICS Oversight and Assurance Framework was agreed in early June 2022 proposing the establishment of three cross-departmental Groups, a HOCS Reference Group, a Public Inquiry Compliance and Assurance Group and a NICS Preparedness and Coordination Group, along with individual departmental preparedness teams. The broad purpose of this Framework was to ensure coordinated approach in relation to:

- Full compliance and participation;
- A collaborative relationship;
- Proper disclosure;
- Effective preparation by witnesses; and
- Adherence to the Inquiry's requirements on handling of documentation.

1.4.5 The draft Terms of Reference for the COVID-19 Inquiry was approved by the Prime Minister in late June 2022 and subsequently 'Rule 9 Requests' were made at a departmental level for information to be provided to the Inquiry (this was not completed as a NICS exercise as each NICS department is an entity in its own right with its own Accounting Officer). Each of these Requests was tailored to the role the department will play in the Inquiry, however we understand that it has been conveyed in Requests that communications may be requested encompassing emails, text messages and WhatsApp messages (on both government and private or personal devices).

NI Executive Ministers and SpAD NICS Devices

1.4.6 To enable Ministers and SpADs to undertake their roles, they are issued with a NICS laptop, a NICS smartphone and usually an NICS tablet. These are procured through IT Assist (part of the Department of Finance) who provide common IT systems and services for the NICS and this process is triggered by Private Office staff completing a service request, forwarded to IT Assist. When Ministers and SpADs no longer require these devices, they are usually returned to IT Assist for reallocation or disposal and this action is similarly triggered by Private Office staff completing a service request, forwarded to IT Assist.

1.5 Work Undertaken

1.5.1 A comprehensive review of relevant NICS policies, procedures, guidance and processes in place during the period of time that the devices were returned has been completed. We also reviewed relevant NI Assembly documents such as the Ministerial Pledge of Office to clarify the roles and responsibilities of Ministers in relation to the retention of official information. We also sought to identify what, if any, further policies, procedures, guidance and processes were issued by departments during this period in relation to retention of information held on mobile devices for the upcoming COVID-19 Inquiry (see **Annex B** for a full list of policies, procedures, guidance and processes reviewed).

1.5.2 29 fact finding interviews across the period 23rd October 2023 to 21st November 2023 with staff who held relevant Private Office posts have been completed. The purpose of these interviews was to gain an understanding of what process Private Offices undertook to secure the return of the mobile devices, how the mobile devices were handled on their return and to establish what steps were taken to identify and/or retain relevant information to the Inquiry on these devices.

1.5.3 The Investigation Team conducted a series of visits to secure mobile devices held by departmental Private Offices as well as engaging with IT Assist to locate mobile devices returned to them by Private Office staff on behalf of Ministers and SpADs.

1.5.4 The Investigation Team also engaged with each department to better understand what actions were taken to ensure that relevant electronic evidence was identified and preserved for the then anticipated COVID-19 Inquiry.

2. EXECUTIVE SUMMARY

2.2 Key Findings and Conclusions

2.2.1 We have set out our key findings and conclusions below:

- The Investigation Team identified that 68 mobile devices had been held by 39 Ministers and SpADs (36 smartphones and 32 iPads) during the relevant period (in a number of instances devices were inherited/reallocated from previous incumbents of the role). The Investigation Team located and secured 44 of these devices and 1 SIM card (24 smartphones, 20 iPads) (See **Annex A** for full details). The Investigation Team did not activate any of the secured devices in order to preserve the integrity of these devices and any potential information retained on them and as a result we have been unable to establish the status with certainty. However based on our investigative work including discussions with relevant staff we have made an assessment on the status of each device at the time when they were returned by Ministers and SpADs and also their subsequent status on being secured by the Investigation Team.

  Assessment of status of devices **at time of return** to Private Offices

  - 4 smartphones have been assessed as being returned 'Unused';
  - For 20 of the mobile devices, the status of these devices has been assessed as 'Reset' at their time of return;
  - For 27 of the mobile devices, the status of these devices has been assessed as 'Not reset' at their time of return;
  - 1 mobile device has been assessed as 'Partially reset' as the email account was removed from a tablet prior to return; and
  - For 16 of the mobile devices, the status of these devices has been assessed as 'Unknown' at their time of return as there is insufficient information to make a reasonable assessment at this time.

Assessment of **current status** of devices secured by the Investigation Team

- For 19 of the 44 secured devices the current status of these devices has been assessed as 'Reset';
- For 16 of the 44 secured devices the current status of these devices has been assessed as 'Not reset'; and
- For 9 of the 44 secured devices the current status of these devices has been assessed as 'Unknown' as there is insufficient information to make a reasonable assessment at this time.

- The Investigation Team considers that Private Office staff operated broadly in line with the overarching NICS policies, procedures, guidance and processes in place in their handling of mobile devices returned by Ministers and SpADs. We noted that actions taken by Private Offices in relation to these devices were split along two lines, with approximately half of the devices returned to IT Assist after being relinquished by Ministers and SpADs, and the other half being retained in Private Offices without returning them to IT Assist (mobile devices returned to IT Assist are routinely reset and reallocated or destroyed (depending on their age and condition)). If the relevant policy had been strictly adhered to (NICS Mobile Device Security Policy), all devices should either have been immediately returned to IT Assist or immediately reallocated to other individuals within the Private Office team. However the Investigation Team has accepted the explanation that the purpose of Private Offices retaining the devices was to allow speedy reallocation, in the reasonable expectation at that time of the NI Executive being re-formed. We also note that this action has led to a significant number of these devices being recovered by the Investigation Team in the state that they were returned to staff, potentially allowing for further analysis.

- The Investigation Team also accepts that IT Assist staff operated in line with the overarching NICS policies, procedures, guidance and processes in place in their handling of mobile devices, previously issued to Ministers and SpADs, returned by Private Offices. However, in actioning the service requests raised by the Private Offices, the vast majority of devices returned to IT Assist were reset in line with standard operating procedures at that time and as a result this may

have inadvertently led to potentially relevant information on these devices being unavailable for further analysis.

- We consider that in line with the overarching NICS Records Management Policy and NI Executive Codes of Conduct, it is clearly each individual's responsibility (whether Minister, SpAD or NICS staff) to ensure that all relevant official information is extracted and retained on Content Manager (CM), the official Electronic Document and Records Management System (EDRMS) of the NICS. Furthermore, any official records created using collaborative systems identified for retention must also be extracted and retained on CM (examples of collaborative systems given in the relevant policy are Microsoft 365 or WhatsApp). In this particular instance, the potential deficiency in disclosure material relates to non-retained communications by Ministers and SpADs on collaborative systems such as text messages / WhatsApp messages from smartphones. Therefore the onus should have been on the relevant Minister or SpAD to have ensured that any relevant communications were retained on CM or flagged for retention to their Private Office staff contemporaneously.

- The Investigation Team consider that as an effective EDRMS (in the form of CM) has been established for the NICS supported by records management policies, guidance and procedures and training, it was reasonable for senior managers when undertaking the disclosure exercise to focus on identifying and retrieving relevant information from CM in the first instance. No supplementary NICS-wide policies, procedures, guidance or processes were issued to staff specifically relating to information held on mobile devices for the upcoming COVID-19 Inquiry, however we noted that departments reminded staff of the need to retain all relevant information for the upcoming Inquiry, and in some instances this included providing guidance for saving information generated from smartphones. However, it is also clear that there is a lack of specific guidance in the use of certain smartphone apps such as WhatsApp to conduct official business, in areas such as what discussions are permissible, should these groups be disclosed or controlled in some way, what audit trails should be maintained or even how long should conversations be retained before deletion

(either discretionary or automated). We would note again that the overarching policy requires all official records to be retained on CM.

3. DETAILED FINDINGS

3.1 Objective 1: To physically locate and secure the relevant mobile devices

3.1.1 The Investigation Team conducted a series of visits to secure mobile devices held by departmental Private Offices as well as engaging with IT Assist to locate mobile devices returned to them by Private Office staff on behalf of Ministers and SpADs.

Number of Mobile Devices Recovered

3.1.2 From a possible total of 68 mobile devices previously held by 39 Ministers and SpADs (36 smartphones and 32 iPads), the Investigation Team located and secured 44 devices and 1 SIM card (24 smartphones, 20 iPads). Of this total, 36 devices and 1 SIM card had been retained by Private Offices at that time (21 smartphones, 15 iPads) and the remaining 8 devices (3 smartphones and 5 iPads) had been returned to IT Assist on or around when they were relinquished by outgoing Ministers and SpADs. For the devices returned to IT Assist, this was actioned through the completion of a service request by the Private Office. Once actioned, these devices were returned to IT Assist where all but the 8 instances stated above, the devices were reset before either being reallocated or destroyed.

Assessment of Status of Mobile Devices Recovered

3.1.3 The Investigation Team confirmed that of the 8 devices held by IT Assist, 2 of them (both smartphones) had not been reset by IT Assist on return. Of the remaining 36 devices that had been retained by Private Offices, we have not been able to establish with certainty how many of these devices were reset prior to being handed over to Private Office staff to preserve the integrity of these devices and any information retained on them. However, based on our investigative work including discussions with relevant staff we have made an assessment[1] on the status of each device at the time when they were returned by Ministers and SpADs and also their subsequent status on being secured by the Investigation Team:

[1] Please note that this is an assessment and not a statement of fact and is based on our investigative work including discussions with relevant staff

Assessment of status of devices **at time of return** to Private Offices

- 4 smartphones have been assessed as being returned 'Unused';
- For 20 of the mobile devices, the status of these devices has been assessed as 'Reset' at their time of return;
- For 27 of the mobile devices, the status of these devices has been assessed as 'Not reset' at their time of return;
- 1 mobile device has been assessed as 'Partially reset' as the email account was removed from a tablet prior to return; and
- For 16 of the mobile devices, the status of these devices has been assessed as 'Unknown' at their time of return as there is insufficient information to make a reasonable assessment at this time.

Assessment of **current status** of devices secured by the Investigation Team

- For 19 of the 44 secured devices the current status of these devices has been assessed as 'Reset';
- For 16 of the 44 secured devices the current status of these devices has been assessed as 'Not reset'; and
- For 9 of the 44 secured devices the current status of these devices has been assessed as 'Unknown' as there is insufficient information to make a reasonable assessment at this time.

A more detailed breakdown of the mobile devices recovered along with our assessment of their status when returned to Private Offices has been set out in **Annex A**.

3.2 Objective 2: Establish what mobile device or relevant policies, procedures, guidance and processes were in place across the NICS at the time of the devices being returned

3.2.1 The Investigation Team has attempted to set out the policies, guidance, procedures, and processes relevant to the use of mobile devices as well as those that frame how official information is managed and retained across the NICS. We have then summarised how this relates to the roles and responsibilities of Ministers, SpADs and NICS staff and what behaviour should be expected from them. It should also be noted that in line with overarching strategic policy requirements, all departments have established their own policies, guidance, procedures, and processes to support and supplement the NICS strategic policies documented below. Given the time constraints placed around this investigation it would not be feasible to drill down to undertake a full policy review across all departments, however we consider that the work completed by the Investigation Team in this area is sufficient to demonstrate that there are adequate strategic policies, guidance, procedures, and processes to allow for reasonable conclusions to be drawn around how official information should be managed as well as expected behaviours for Ministers, SpADs and NICS staff. A full list of all policies, guidance, procedures, and processes reviewed by the Investigation Team can be found at **Annex B** (not all of these documents were found to be relevant to the investigation but have been included for transparency).

Guidance in relation to Mobile Devices

NICS Mobile Device Security Policy

3.2.2 A NICS Mobile Device Security Policy has been in place since 2012 and was most recently updated in June 2023. The Investigation Team reviewed previous iterations of this policy covering the period of the investigation and any amendments do not change the core principles documented below. The policy applies to all NICS approved and supported mobile devices (this includes smartphones and tablets) issued by the NICS and all users of these devices must comply with the policy. The policy is primarily focused on the security of these devices and in the Introduction section the policy states "*This security policy provides the reasoning and processes for minimising the risk associated with handling (accessing, storing, processing,*

transmitting, discussing or recording) Official information on mobile devices. Its purpose is to ensure that staff members are fully aware of the security required to protect assets, in particular sensitive or personal information".

3.2.3 Section 3 clearly states the personal responsibilities for users of NICS issued mobile devices. These include:

- *"Users are responsible for the physical security of all mobile devices provided for work purposes, AND for the information stored on them;*
- *The mobile device remains the property of the NICS and must only be used in accordance with official guidelines;*
- *Where a mobile device is no longer required by its original recipient, it must be returned to IT Assist for secure erasure, reloading of software, re-encryption and redeployment. It must not be retained by the Branch as a spare; and*
- *In exceptional circumstances there may be a requirement for a mobile device to be reallocated to another member of staff within a Branch……It is also their responsibility to ensure that this is recorded in an auditable, business process and that IT Assist are informed."*

NICS Staff Handbook Standards of Conduct

3.2.4 Paragraph 32.2 states "*On resignation or retirement from the NICS, you must return your security/official identity passes, together with any other official property that was issued to you*". This document also restates the requirements of the NICS Code of Ethics (see above).

Overarching Records Management Principles and Guidance

3.2.5 Up to 2005 all NICS departments had a purely paper-based records management system. At this point the NICS decided to utilise an EDRMS to capture, store, manage, and retrieve documents and records. The NICS initially selected TRIM as the software platform for its corporate EDRMS and TRIM subsequently became CM after the software was acquired by Microfocus.

NICS Records Management Policy

3.2.6 The use of CM as the EDRMS has been codified in a number of policies, the most relevant being the NICS Records Management Policy V2.0 (covering the period November 2020 to November 2023). This is a NICS strategic policy and applies to the management of all documents and records, in all formats or media, created or received by NICS Departments in the conduct of their business activities. It also applies to all staff, contractors, consultants and third parties who may be given access to NICS documents and records and information processing facilities.

3.2.7 The policy states that "*all employees of the NICS (permanent and temporary), contractors, consultants and secondees must ensure that the records for which they are personally responsible are complete and accurate. They must also ensure that records are maintained and disposed of in accordance with the Departmental records management policies and procedures*".

3.2.8 Within this policy CM is mandated as the corporate repository for the majority of information created and received by each NICS department in the course of their duties and CM is the mandated system for the purpose of this investigation. Furthermore this policy requires that any records created by other collaborative systems identified for retention must be extracted and retained on CM (examples of collaborative systems policy are Microsoft 365 or WhatsApp).

It is acknowledged that there may be official information held on other systems, such as line of business systems as well as a small number of shared drives, however this is not material to this investigation.

NICS Official Information Held in Non-Corporate Channels Policy

3.2.9 This policy was implemented from June 2022, therefore would be applicable to the majority of Ministers and SpADs as they remained in position until end of October 2022. The policy defines non-corporate channels and outlines records management responsibilities if these channels are used. In defining non-corporate channels, the following communication channels are provided as an illustration of what may be considered to fall within the policy:

- Personal email accounts e.g., Hotmail, Gmail, ProtonMail or Yahoo Mail;

- Private messaging accounts e.g., WhatsApp, Signal or Telegram;
- Direct messages sent on apps such as Twitter or via Facebook messenger; and
- Personal mobile devices, including text messages on mobile phones and voice recordings.

3.2.10 The policy mandates that information relating to departmental business should be recorded on CM and erasing, destroying or concealing information with the intention of preventing its disclosure is an offence. It also mandates that as a rule, civil servants should not be processing official information using anything other than official devices and official channels. Where this is not possible, the official information must be saved onto corporate systems as quickly as possible, e.g., Outlook or CM, and removed as quickly as possible from non-corporate channels.

NICS code of Ethics

3.2.11 Following the RHI Inquiry, the NICS Code of Ethics was revised and reissued in February 2020. This Code sets out a number of standards focused around NICS core values of integrity, honesty, objectivity and impartiality. Of particular interest is section 8 that states "*You must…..keep accurate official records, including minutes of ministerial meetings, and handle information as openly and transparently as possible within the legal framework*".

NI Executive Ministers and SpAD Specific Policies, Procedures, Guidance and Processes

3.2.12 All Ministers (including the FM and dFM) are required to follow the Ministerial Code which sets out the rules and procedures for the exercise of the duties and responsibilities of Ministers and Junior Ministers of the Northern Ireland Assembly. Ministers are also required to comply with the Ministerial Code of Conduct as well as the Seven Principles of Public Office. This is completed through affirming the Pledge of Office. They are also required to comply with the NI Executive Guidance for Ministers in the Exercise of their Responsibilities.

3.2.13 SpADs are temporary civil servants and as well as being required to comply with the normal NICS policies, procedures, guidance and process documented above for

normal civil servants, there are a number of further pieces of guidance that they are required to comply with such as the Code of Conduct for Special Advisers 2020 and the NICS Records Management Protocol for Special Advisers 2020.

3.2.14 Furthermore Ministers and SpADS are subject to the Functioning of Government (Miscellaneous Provisions) Act NI 2021 that was passed by the NI Assembly on 02 February 2021 and received Royal Assent on 22 March 2021. The Act contains important provisions regarding records of relevant ministerial meetings and the presence of civil servants at meetings that Ministers and Special Advisers may have with people outside the department. We have set out below key extracts from these documents.

Northern Ireland Executive Ministerial Code (2006)

3.2.15 The Ministerial Code sets out the rules and procedures for the exercise of the duties and responsibilities of Ministers and junior Ministers of the Northern Ireland Assembly. It includes the Pledge of Office as well as the requirements to follow the Ministerial Code of Conduct and the seven principles of public life.

Ministerial Code of Conduct

3.2.16 This Code sets out nine requirements including to:

- Observe the highest standards of propriety and regularity involving impartiality, integrity and objectivity in relationship to the stewardship of public funds; and
- Ensure that all reasonable requests for information from the Assembly, users of services and individual citizens are complied with; and
- That departments and their staff conduct their dealings with the public in an open and responsible way;

Seven Principles of Public Office

3.2.17 The two principles primarily relevant to this investigation are those relating to accountability and openness:

- Accountability: Holders of public office are accountable for their decisions and actions to the public and must submit themselves to whatever scrutiny is appropriate to their office; and
- Openness: Holders of public office should be as open as possible about all the decisions and actions that they take. They should give reasons for their decisions and restrict information only when the wider public interest clearly demands.

NI Executive Guidance for Ministers in the Exercise of their Responsibilities

3.2.18 This guidance, issued in March 2020, sets out the procedures to be followed by Ministers in the effective exercise of their duties and responsibilities and in circumstances where those duties and responsibilities may engage with personal, party political or business interests. The guidance applies to all members of the Executive Committee and to Junior Ministers. The guidance states at paragraph 7.1 that "*Ministers must at all times adhere to the rules regarding the management of official information*" and further states at paragraph 7.3 that "*Ministers must use official email systems for all communications relating to official business. Exceptionally, where this is not possible, the Minister must copy any message to their official email account. Information generated in the course of government business must be handled in accordance with the requirements of the law (including the Freedom of Information Act 2000 (FoI), the Environmental Information Regulations 2004 (EIR), GDPR and Public Records Act (NI) 1923), regardless of how it is communicated*".

NICS Records Management Protocol for Special Advisers (2020)

3.2.19 The protocol sets the guidelines around transparency and record keeping that SpADs must adhere to and references the Code of Conduct for Special Advisors (see below). The protocol clearly states that SpADs must keep accurate official records and the focus of the guidance in the protocol is mainly in relation to email and the use of CM. However the Protocol states at paragraph 11 that "*Use of private email accounts are an exceptional basis as provided for in the Code of Conduct, or other media used for official business will still form part of the official record and be subject to FoI, etc.".*

Code of Conduct for Special Advisers 2020

3.2.20 This Code includes guidelines around transparency and record keeping, stipulating that:

- SpADs must keep accurate official records, including minutes of relevant meetings, and handle information as openly and transparently as possible within the legal framework;
- SpADs must use official email systems for communications relating to official business. Exceptionally, where this is not possible, the SpAD must copy any message to their official email account; and
- Information generated in the course of government business must be handled in accordance with the requirements of the law (including the Freedom of Information Act, GDPR/ Data Protection Act, and the Public Records Act), regardless of how it is communicated.

Functioning of Government (Miscellaneous Provisions) Act NI 2021

3.2.21 The Functioning of Government (Miscellaneous Provisions) Act NI 2021 (FoG Act) contains important provisions regarding maintaining records of relevant ministerial meetings and the presence of civil servants at meetings that Ministers and SpADs have with people outside the department.

3.2.22 Guidance was issued to Minsters and SpADS by HOCS in March 2021 and of particular note are paragraphs 3 and 4 which state: "*Ministers and Special Advisers should actively facilitate the recording of meetings and decisions. All relevant meetings must be recorded by a civil servant and the written record retained in line with the Department's retention and disposal schedule. Permanent Secretaries will be provided with assurance from the Private Secretary that arrangements are in place for this work to be completed*". The document goes on to state in paragraph 7 that: "*The arrangements must additionally ensure that all ministerial decisions in respect of official business are recorded properly, whether taken in a pre-arranged meeting or not*".

Summary of the impact these principles, structures and systems have on how Ministers, SpADs, NICS staff and internal functions should act in relation to their use of NICS issued mobile devices and the information generated by them.

3.2.23 Requirements of Ministers

- Users are responsible for the physical security of all mobile devices provided for work purposes, AND for the information stored on them;
- NICS issued mobile devices remain the property of the NICS and must only be used in accordance with official guidelines;
- All staff, contractors, consultants and third parties who may be given access to NICS documents and records and information processing facilities must ensure that the records for which they are personally responsible are complete and accurate. They must also ensure that records are maintained and disposed of in accordance with the Departmental records management policies and procedures;
- Any records created by other collaborative systems identified for retention must be extracted and retained on CM (examples of collaborative systems policy are Microsoft 365 or WhatsApp);
- Ministers must at all times adhere to the rules regarding the management of official information;
- Ministers must use official email systems for all communications relating to official business. Exceptionally, where this is not possible, the Minister must copy any message to their official email account. Information generated in the course of government business must be handled in accordance with the requirements of the law (including the Freedom of Information Act 2000 (FoI), the Environmental Information Regulations 2004 (EIR), GDPR and Public Records Act (NI) 1923), regardless of how it is communicated;
- Ministers must observe the highest standards of propriety and regularity involving impartiality, integrity and objectivity in relationship to the stewardship of public funds;

- Ministers must ensure that all reasonable requests for information from the Assembly, users of services and individual citizens are complied with; and that departments and their staff conduct their dealings with the public in an open and responsible way;
- Accountability: Holders of public office are accountable for their decisions and actions to the public and must submit themselves to whatever scrutiny is appropriate to their office; and
- Openness: Holders of public office should be as open as possible about all the decisions and actions that they take. They should give reasons for their decisions and restrict information only when the wider public interest clearly demands.

3.2.24 Requirements of NICS Staff (including SpADs)

- All staff, contractors, consultants and third parties who may be given access to NICS documents and records and information processing facilities must ensure that the records for which they are personally responsible are complete and accurate. They must also ensure that records are maintained and disposed of in accordance with the Departmental records management policies and procedures;
- CM is mandated as the official EDRMS of the NICS and this should be the primary repository of official information;
- Any records created by other collaborative systems identified for retention must be extracted and retained on CM (the official EDRMS);
- Users are responsible for the physical security of all mobile devices provided for work purposes, AND for the information stored on them;
- NICS issued mobile devices remain the property of the NICS and must only be used in accordance with official guidelines;
- Where a mobile device is no longer required by its original recipient, it must be returned to IT Assist for secure erasure, reloading of software, re-encryption and redeployment, or, in exceptional circumstances there may be a requirement for a mobile device to be reallocated to another member of staff within a Branch;

- Information relating to departmental business should be recorded on CM and erasing, destroying or concealing information with the intention of preventing its disclosure is an offence;
- Civil servants should not be processing official information using anything other than official devices and official channels. Where this is not possible, the official information must be saved onto corporate systems as quickly as possible, e.g., Outlook or CM, and removed as quickly as possible from the non-corporate channels;
- NICS staff must keep accurate official records, including minutes of ministerial meetings, and handle information as openly and transparently as possible within the legal framework; and
- On resignation or retirement from the NICS, you must return your security/official identity passes, together with any other official property that was issued to you.

3.2.25 Requirements for SpADs Over and Above Normal NICS Policies, Guidance and Procedures

- SpADs must keep accurate official records, including minutes of relevant meetings, and handle information as openly and transparently as possible within the legal framework;
- SpADs must use official email systems for communications relating to official business. Exceptionally, where this is not possible, the SpAD must copy any message to their official email account;
- Information generated in the course of government business must be handled in accordance with the requirements of the law (including the Freedom of Information Act, GDPR/ Data Protection Act, and the Public Records Act), regardless of how it is communicated; and
- Use of private email accounts are an exceptional basis as provided for in the Code of Conduct, or other media used for official business will still form part of the official record and be subject to Freedom of Information, etc.

3.3 Objective 3: Establish what specific guidance or instructions have been issued relating to retention of information held on mobile devices for the Inquiry

3.3.1 As per paragraph 1.4.2 above, in September 2021 and October 2022 the Head of the Civil Service (HOCS) wrote to all NICS Permanent Secretaries reiterating the need to take steps to assure themselves that Departments and ALBs would be ready to meet their obligations to provide relevant records, information and data to the Inquiry. We noted that in the September 2021 communication HOCS advised "*….we will be issuing a note to all staff to reinforce the importance of rigorously applying these processes in relation to issues which may be relevant to a COVID inquiry*". The Investigation team confirmed that subsequent communications were not issued by HOCS during the relevant period. We also noted that no further supplementary NICS-wide policies, procedures, guidance or processes were issued to staff specifically relating to information held on mobile devices for the upcoming COVID-19 Inquiry, however we noted that departments reminded staff of the need to retain all relevant information for the upcoming Inquiry, and in some instances this included providing guidance for saving information generated from smartphones. This was confirmed through our fact finding interviews with Private Office staff who acknowledged that they were generally aware of an upcoming COVID-19 Inquiry and were confident that their existing records management practices would allow all relevant information to be identified.

3.3.2 The Investigation Team engaged with each department to better understand what actions were taken to ensure that relevant electronic evidence was identified and preserved for the then anticipated COVID-19 Inquiry (e.g. email and other electronic communications such as text messages, WhatsApp messages and voicemail, word-processed documents and databases, and documents stored on portable devices such as memory sticks and mobile phones). We are content that from autumn 2021 onwards departments allocated significant resources to ensure adequate and effective systems were established to be properly prepared to meet their obligations for the forthcoming Inquiry and that there was regular monitoring of the progress by senior managers within each department and across the NICS through the

establishment and operation of the NICS Oversight and Assurance Framework. It is also clear that management considered CM as the main source for identifying information relevant to the Inquiry which is understandable given that CM is the mandated repository for official information.

3.3.3 During this period, there was a reasonable expectation that in line with the overarching records management policies, all official information relevant to the upcoming Inquiry should have been saved to CM and therefore would be retrieved from CM. We would also note that there may have been a potential gap between what the NICS and the CoVID-19 Inquiry would consider 'information relevant to the Inquiry', in that the information requirements of the COVID-19 Inquiry would seem to be in some instances requesting additional information differing from the usual official business retention standard of the NICS and this may go some way to explain how the current situation has arisen in relation to the treatment of these mobile devices.

3.4 Objective 4: Establish what steps (if any) were taken to identify and/or retain relevant information on the mobile devices

3.4.1 We have been advised by Private Office staff that they did not attempt to access the devices returned by Ministers and SpADs to identify and/or retain relevant information and instead either returned them to IT Assist or stored them securely with the view of quickly reallocating them to new Ministers and SpADs. In a small number of instances devices were switched on to see if they were still working, however once this was established they were switched off again. We have been advised by one department that the Minister's and SpAD's smartphones were examined for copies of their WhatsApp/text messages, however this exercise was not completed by the Private Office; the conclusions from this review were that the devices had not been used for any decision-making process or discussing business decisions. We consider that any further activity of this kind should be carefully planned and undertaken to ensure that the integrity of all devices examined is maintained, including maintaining any chain of custody linked to the devices.

3.4.2 IT Assist advised that they accessed devices still retained by them to establish whether they had been reset but have not attempted to retrieve and/or retain any relevant information from the devices.

3.4.3 The investigation Team has not attempted to establish with certainty how many of these devices were reset prior to being handed over to Private Office staff, nor have we attempted to identify and/or retain any relevant information on these devices. The purpose of not accessing the devices is to preserve the integrity of these devices and any potentially relevant information on them.

3.4.4 Management may wish to have the recovered mobile devices further analysed to confirm the current status of each device and also to confirm what, if any, further relevant information could be extracted from these devices.

3.4.5 We also note that any proven allegations of non-compliance with the COVID-19 Inquiry connected to non-disclosure or destruction of information potentially held on these devices could be deemed criminal offences under the Inquiries Act (2005),

and if any allegations of this kind were to be properly investigated to the required criminal standard it would be crucial to preserve the integrity of the devices, including maintaining any chain of custody linked to the devices (as per paragraph 3.4.1 above).

3.5 Objective 5: Document the circumstances that led to a number of mobile devices being erased/reset prior to being returned or on return, including whether this was in line with the relevant policies, procedures and guidance in place at that time

3.5.1 The fact finding interview process took place during the period 23rd October 2023 to 21st November 2023 and 29 individuals were interviewed across all NICS Private Offices and across grades from AO to Grade 5 Private Secretary. The purpose of this exercise was to:

- Establish what steps (if any) were taken to identify and/or retain relevant information on the mobile devices returned by Ministers and Special Advisors; and
- Document the actions taken following the mobile devices being returned to the NICS by Ministers and Special Advisors.

3.5.2 We have structured the results of our discussion into two topics:

- Retrieval of mobile devices from Ministers and SpADs; and
- Treatment of mobile devices retrieved from Ministers and SpADs including any actions to extract information from returned devices.

Retrieval of Mobile Devices from Ministers and SpADs

3.5.3 It is clear from the accounts given by Private Office staff that when the NI Assembly collapsed they were all aware of the need to retrieve NICS issued equipment from outgoing Ministers and SpADs as quickly as possible. There was no established procedure within any of the Private Offices for completing this activity, however it is clear that the requirements set out in the NICS Mobile Device Security Policy were used as the basis for the actions of staff involved in the process and was largely described as using 'custom and practice'. There was also no mandated location for this process and the handover of the devices happened at various locations, for example private residences of outgoing Ministers, Parliament Buildings, Private Offices or even the back seat of Ministerial cars.

We note that Ministers are not required to confirm that they have returned all NICS devices, to declare the status of the devices returned, or confirm that all relevant

official information has been saved to CM (or flagged for saving to Private Office staff) and this is an area that management may wish to strengthen. In theory, as SpADs are temporary civil servants, a Leaver's Checklist form could have been completed (a form that all NICS staff are required to complete when they leave the employments of the NICS), part of which confirms the return of all NICS equipment and security passes. As a result there were few direct records of the handover of the mobile devices from Ministers to Private Office staff and only a few instances where the SpAD was asked to complete a Leaver's Checklist. There were subsequent records retained relating to these devices being returned to IT Assist or reallocated within Private Offices.

Treatment of Mobile Devices Retrieved From Ministers and SpADs

3.5.4 We noted that actions taken by Private Offices in relation to these devices were split along two lines, with approximately half of the devices returned to IT Assist and the other half being retained in Private Offices for a significant period without returning them to IT Assist. Private Office staff consistently explained that the reason for holding on to these devices in the short-term was to allow speedy reallocation in the reasonable expectation at that time of the NI Executive being re-formed. When this did not happen as soon as envisaged, as no time limit had been set on how long these devices should have been retained for, they remained in the custody of the Private Offices. We would note that this action has led to a significant number of these devices being recovered by the Investigation Team in the state that they were returned to Private Office staff, potentially allowing for relevant information to now be extracted.

3.5.5 Private Office staff advised that they did not attempt to access the devices returned by Ministers and SpADs except in a small number of instances where the devices were checked to see if they were still operational and staff confirmed that they did not attempt to identify and/or retain relevant information on the devices. This was understandable given that NICS staff are advised not to access any NICS device that has not been issued to them.

3.5.6 For the devices returned to IT Assist, this was actioned through the completion of a service request by the Private Office. Once actioned, these devices were returned to IT Assist where in all but 8 instances, the devices were reset before either being reallocated or destroyed in line with the NICS Mobile Device Security Policy. Management advised that records of these service requests had been retained on CM.

3.5.7 In a small number of instances, devices were reallocated to Private Office staff. For example, in one instance an iPad was reallocated to a Private Office staff member who was undergoing medical treatment and this allowed them to continue to access their work emails whilst offsite, in a location without Wi-Fi. In these instances service requests were issued to IT Assist to facilitate the change of ownership. This was understandable as the Private Office was paying a monthly fee for the device and instead of incurring a further monthly cost by procuring a new device, and given the ongoing budgetary pressures currently faced by the NICS, it was a reasonable decision to reallocate a device already in their possession.

3.5.8 Our fact finding interviews also confirmed that Private Office staff were aware that CM should be the main repository of official information. Furthermore staff stressed that they were aware of the need to keep a complete and accurate record of official Private Office business. It is clear that the results of the RHI Inquiry and also the requirements resulting from the FoG Act 2021 had shaped their thinking in this area as this was repeatedly quoted as justifications for reminding Ministers and SpADs to ensure effective records management was maintained. Staff also stressed that they regularly asked Ministers to flag communications that would require saving over and above the normal routine documentation that Private Office took responsibility over (Ministers had no direct access to CM).

3.5.9 We noted that there was a lack of consistency across the NICS in the working practices that Ministers used and this regularly impacted on the efficiency of their records management function. For example, some Ministers refused to use the NICS issued smartphones and instead used another smartphone for official

business and other Ministers insisted on working off a primarily hard copy system, where all relevant papers had to be printed off for hand written amendments and approvals. Management may wish to revisit this area and provide some further guidance to Ministers, perhaps considering mandating what equipment will be used for official business and also the primary method of communication for conducting official business, such as mandating an electronic first methodology that the rest of the NICS are required to use.

Annex A

Summary of Minister and SpAD Mobile Devices

Dept	Minister / SpAD	Devices issued	Investigation Team Assessment[2] of status of device at time of return to Private Office (unused / reset / partially reset/ not reset / unknown / unused)	Devices retrieved by Investigation Team (Y/N)	Investigation Team Assessment of current status of retrieved devices (reset / not reset / unknown)
TEO	FM Arlene Foster	Smartphone	Unused	**Partial Y**. SIM card retrieved. Phone reallocated within Private Office.	Smartphone reset and reallocated. SIM card available.
		iPad	Not reset	**Y** (reset by IT Assist and reallocated to Minister Givan)	N/A
	FM Paul Givan	Smartphone	Not reset	**Y**	**Not reset**
		iPad	Not reset	**Y**	**Not reset**
	dFM Michelle O'Neill	Smartphone	Reset	**Y**	**Reset**
		iPad	Reset	**Y**	**Reset**
	SpAD Philip Weir	Smartphone	Not reset	**Y**	**Not reset**
		iPad	Not reset	**Y**	**Not reset**

[2] **Please note that this is an assessment and not a statement of fact and is based on our investigative work including discussions with relevant staff**

	SpAD Richard Bullick	Smartphone	Not reset	**Y** (reset by IT Assist and reallocated to SpAD Pengelly)	N/A
		iPad	Not reset	**Y** (reset by IT Assist and reallocated to SpAD Pengelly)	N/A
	SpAD Emma Little Pengelly	Smartphone	Unknown	**Y**	**Unknown**
		iPad	Unknown	**Y**	**Unknown**
	JM1 Gordon Lyons / Gary Middleton	Smartphone	Unknown	**Y**	**Unknown**
		iPad	Unknown	**Y**	**Unknown**
	JM2 Declan Kearney	Smartphone	Reset	**Y**	**Reset**
		iPad	Unknown	**Y**	**Unknown**
	SpAD Kim Ashton / Lee Reynolds	Smartphone	Not reset	N	N/A
		iPad	Not reset	**Y**	**Not reset**
	SpAD John Loughran	Smartphone	Reset	**Y**	**Reset**
		iPad	Reset	**Y**	**Reset**
	SpAD Stephen McGlade	Smartphone	Reset	**Y**	**Reset**
		iPad	Reset	**Y**	**Reset**
	SpAD Michelle Canning	Smartphone	Reset	**Y**	**Reset**
		iPad	Reset	N	N/A
	SpAD Dara O'Hagan	Smartphone	Reset	**Y**	**Reset**
		iPad	Reset	**Y**	**Reset**
DOF	Minister Conor Murphy (note: Minister refused smartphone)	iPad	Partially reset (email account removed)	**Y** (reset by IT Assist)	**Reset**
	SpAD Eoin Rooney	Smartphone	Not reset	**Y**	**Not reset**

		iPad	Unknown	**Y** (reset by IT Assist)	**Reset**
DOH	Minister Robin Swann	Smartphone	Not reset	**Y** (reset by IT Assist)	**Reset**
		iPad	Not reset	N (reset by IT assist and reallocated within Private Office)	N/A
	SpAD Mark Ovens	Smartphone	Not reset	**Y**	**Not reset**
		iPad	Not reset	N	N/A
DFC	Minister Deirdre Hargey	Smartphone	Unused	N (reset and disposed of by IT Assist)	N/A
		iPad	Unknown	N	N/A
	Minister Carál Ní Chuilín	Smartphone	Unused	N	N/A
		iPad	Unknown	N (reset by IT Assist and reallocated to SpAD McGinley)	N/A
	SpAD Ronan McGinley	Smartphone	Reset	N	N/A
		iPad	Reset	N	N/A
DAERA	Minister Edwin Poots	Smartphone	Unused	N	N/A
		iPad1	Not reset	**Y** (reset by IT Assist)	**Reset**
		iPad2	Not reset	**Y** (reset by IT Assist)	**Reset**
	Minister Gordon Lyons	Smartphone	Unknown	N	N/A
		iPad	Unknown	N	N/A
	SpAD Mark Beattie	Smartphone	Not reset	N	N/A
		iPad	Not reset	**Y**	**Not reset**
DFI	Minister Nichola Mallon (SDLP)	Smartphone	Not reset	**Y**	**Not reset**
		iPad	Not reset	N	N/A
	Minister John O'Dowd	Smartphone	Unknown	**Y**	**Unknown**
		iPad	Unknown	**Y**	**Unknown**

	SpAD Tanya McCamphill	Smartphone	Unknown	N	N/A
		iPad	Unknown	N	N/A
	SpAD Dara O'Hagan	Smartphone	Reset	**Y**	**Reset**
		iPad	Reset	**Y**	**Reset**
DFE	Minister Dianne Dodds	Smartphone	Not reset	**Y**	**Not reset**
		iPad	Not reset	**Y** (reset by IT Assist and reallocated to Minister Frew)	N/A
	Minister Paul Frew	Smartphone	Not reset	**Y**	**Not reset**
		iPad (from Dodds)	Not reset	**Y** (reset by IT Assist and reallocated to Minister Lyons)	N/A
	Minister Gordon Lyons	Smartphone	Not reset	**Y**	**Not reset**
		iPad (from Dodds)	Not reset	**Y**	**Not reset**
	SpAD Alistair Ross	Smartphone 1	Unknown	**Y**	**Unknown**
		Smartphone 2	Unknown	**Y**	**Unknown**
		iPad	Unknown	**Y** (reset by IT Assist and reallocated within Private Office)	**Reset**
DOJ	Minister Naomi Long	Smartphone	Reset	N (reallocated within Private Office).	N/A
		iPad	Reset	N	N/A
	SpAD Claire Johnson	Smartphone	Reset	**Y**	**Reset**
		iPad	Reset	N (reallocated within Private Office)	N/A
	SpAD Patricia O'Lynn	Smartphone	Reset	N	N/A

		iPad	Unknown	N	N/A
DE	Minister Peter Weir	Smartphone	Not reset	N (reset by IT Assist and disposed of)	N/A
		iPad	Not reset	**Y** (reset by IT Assist and reallocated to Minister McIlveen)	N/A
	Minister Michelle McIlveen	Smartphone	Not reset	**Y**	**Not reset**
		iPad	Not reset	N (reset by IT Assist and reallocated within Private Office)	N/A
	SpAD Peter Martin	Smartphone	Not reset	**Y**	**Not reset**
		iPad	Not reset	**Y**	**Not reset**

Annex B

Codes, Policies, Guidance, Procedures and Processes Reviewed by the Investigation Team:

- Box processes and procedures 2018;
- DOF Good Records Management;
- FOIA s46 code of practice on records management;
- Guide on exporting WhatsApp chats (July 2022)
- Guidance issued by DoF in March 2021 resulting from the Functioning of Government (Miscellaneous Provisions) Act (Northern Ireland) 2021;
- NI Assembly Code of Conduct;
- NI Assembly Ministerial Code of Conduct;
- NI Assembly Pledge of Office;
- NI Assembly Seven Principles of Public Life;
- NICS Code of Ethics;
- NICS Dignity at Work Policy;
- NICS Discipline Policy
- NICS Document Version Control Guidance;
- NICS Email Management Policy;
- NICS guidance on Records Management for Non-Executive Directors (NEDs) and Boardroom Apprentices;
- NICS Guidance on Records management for Special Advisers;
- NICS Guidance: Official information held in non-corporate communication channels;
- NICS Handling information securely
- NICS Microsoft Team Policy;
- NICS Mobile Device Security Policy;
- NICS naming conventions best practice guidance;
- NICS Official information held in non-corporate channels policy
- NICS policy on recording video conferences;
- NICS policy on the use of Sharepoint 2018;
- NICS Protection of information during relocation policy 2018;
- NICS Records Management Governance Framework;

- NICS Records Management Policy;
- NICS records retention and disposal policy;
- NICS Retention and Disposal policy statement;
- NICS Use of electronic communications policy;
- NICS Standards of Conduct Policy;
- NI Executive Guidance for Ministers in the Exercise of their Responsibilities;
- PRONI appraisal policy;
- PRONI Digital Repository Submission guidance;
- PRONI retention and disposal process;
- PRONI retention and disposal schedules;
- PRONI selection policy statement;
- Secure File Transfer Protocol (SFTP) approval process 2018; and
- Special Adviser Appointment Letter.