

10 June 2024

195 Lambton Quay
Private Bag 18-901
Wellington 6160
New Zealand

Scott
fyi-request-26840-be33127b@requests.fyi.org.nz

T +64 4 439 8000
F +64 4 472 9596

OIA 29376

Tēnā koe Scott

I refer to your email of 16 May 2024 in which you request the following under the Official Information Act 1982 (OIA):

"The 2022 update to the NZ Classification System Policy introduced new advisories and requirements for PSR-mandated agencies who hold classified information such as the MFAT.

Relating to this, I would like to request copies of:

- 1. ONE: The MFAT Declassification Policy*
- 2. TWO: The MFAT Declassification Governance Framework*
- 3. THREE: Any MFAT documents that set out criteria for declassifying documents*
- 4. FOUR: If MFAT has made any changes to its regular annual declassification and release program since the release of the new PSR Classification System Policy in 2022, what these changes are*
- 5. FIVE: For the PSR Self-Assessment Reports submitted 2023 and 2024, all answers supplied by MFAT to the questions relating to the implementation of the 2022 Classification System Policy update (including any written answers and attachments included as part of MFAT's answers)"*

The Ministry of Foreign Affairs and Trade (the Ministry) continually works towards meeting the Protective Security Requirements (PSR) as set out on PSR website:

<https://www.protectivesecurity.govt.nz/>

The Ministry regularly releases historical files as part of its declassification programme and has done so for many decades. The Ministry's declassification programme sees records 25 years and older systematically reviewed and declassified, subject to a process to ensure New Zealand's interests are protected. Once declassified, files are then available to access through Archives New Zealand.

You can view the Ministry's media statements about the releases, including lists of the files released, on the Ministry's website:

<https://www.mfat.govt.nz/en/media-and-resources/release-of-hundreds-of-previously-classified-historical-files?m=611143#search:ZGVjbGFzc2lmaWNhdGlvbG9z>

In response to part one of your request for "*The MFAT Declassification Policy*". The Ministry does not have a standalone 'Declassification Policy', therefore this part of your request is refused under section 18(e) of the OIA, as the information does not exist. To note, this is in line with PSR guidance as set out on the PSR website <https://www.protectivesecurity.govt.nz/classification-system/how-to-declassify/>, which states as follows:

"Mandated agencies are required to have an organisational policy and procedures for declassification of classified archival information. This need not exist as a standalone policy and declassification requirements may be easier to include within existing information management policies."

Instead, elements of declassification and requirements under the PSR have been embedded across various other Ministry policies and procedures, such as within the Official Information Act process. The most substantial of these policies and procedures are set out in our response to part three of your request.

The Ministry distinguishes between the declassification of historical records and the declassification of contemporary documents. The majority of information provided below relates to the declassification and release of historical information. Policies and processes relating to the declassification of contemporary documents are currently under review as part of a wider Ministry security policy review project. In respect of the declassification of contemporary documents, only the author, or specific, pre-approved roles, can declassify a document.

In response to part two of your request for "*The MFAT Declassification Governance Framework*". In addition to the information contained in the policies below, the Ministry's Instrument of Delegation states that authority to "Declassify records held within the Ministry or at Archives NZ" is delegated from the Chief Executive to:

- Deputy Chief Executive, People and Operations
- Chief Information Officer
- Chief Data Officer
- Vetting Adviser/Officer.

In response to part three of your request for "*Any MFAT documents that set out criteria for declassifying documents*", please refer to the following annexes for relevant information in scope:

- Annex A – Information policy
- Annex B - Declassification and release of historical information standard
- Annex C - Managing requests for historical classified information.

As noted above, as elements of the declassification process are captured in some small parts of most internal document management policies, only the most substantial policies have been set out above.

In response to part four of your request for "*If MFAT has made any changes to its regular annual declassification and release program since the release of the new PSR Classification System Policy in 2022, what these changes are*", I can advise that there have been no significant changes since

the release of the new PSR Classification System Policy in 2022, however the Ministry's processes were reviewed at that time to ensure they met any new requirements.

Prior to the PSR update in 2022, the Ministry already had a declassification programme in place, and as such was very actively involved in contributing to the material in the updated PSR guidance around declassification programmes.

More broadly speaking, the Ministry's policies are regularly reviewed to ensure they are up to date with relevant legislation and other requirements, however not all reviews result in changes being required to be made.

In response to part five of your request for "*For the PSR Self-Assessment Reports submitted 2023 and 2024, all answers supplied by MFAT to the questions relating to the implementation of the 2022 Classification System Policy update (including any written answers and attachments included as part of MFAT's answers)*", please refer to Annexes D and E for extracts of the Ministry's PSR Self-Assessment Reports for the 2022/23 and 2023/24 years (respectively).

Please note that it is our policy to proactively release our responses to official information requests where possible. Therefore, our response to your request (with your personal information removed) may be published on the Ministry website: www.mfat.govt.nz/en/about-us/contact-us/official-information-act-responses/

If you have any questions about this decision, you can contact us by email at: DM-ESD@mfat.govt.nz. You have the right to seek an investigation and review by the Ombudsman of this decision by contacting www.ombudsman.parliament.nz or freephone 0800 802 602.

Nāku noa, nā



Sarah Corbett
for Acting Secretary of Foreign Affairs and Trade

Annex A – Information Policy

Purpose

The purpose of this policy is to ensure that data and information are well-managed and well-used, and can be used to provide a full evidentiary history of Ministry decisions and inform its operational and policy decision-making.

This policy must be read in conjunction with the related standards; Declassification and release of historical information standard, History and heritage collection development standard, Official Information Act standard, and others in development.

Application

This policy will apply to all Ministry of Foreign Affairs and Trade staff, contactors or contracted providers (including vendors) who create, manage or share information with the Ministry.

It encompasses data and information in all formats, including intranet, website and social media content. It includes records.

In this policy the term "information" will be used to include data, content and information.

Responsibilities

The following roles have specific responsibilities under this policy; details are outlined later in the policy:

Role	Responsibility
Executive Sponsor, Public Records Act 2005 (Deputy Chief Executive, People and Operations)	<ul style="list-style-type: none"> • Ensure that the strategy and policy adopted by the Ministry supports information and records management • Ensure that strategic and operational planning aligns information and records management with the corporate objectives and business activities of the Ministry; and information and records management is integrated into processes, systems and services • Ensure that the resources needed to support information and records management are known and sought in funding decisions; and that staff with appropriate skills are available to implement information and records management strategies • Ensure that information and records management is monitored and reviewed to ensure that it is implemented
Chief Data Officer	<ul style="list-style-type: none"> • Ensure compliance with organisational information policies, legislation and other government requirements • Oversee the design, implementation and maintenance of systems, tools, policies, processes and practices that operationalise and are compliant with this policy and that meet business requirements • Establish any required procedures, guidelines or practices needed to ensure the integrity, quality and effective use of Ministry information assets • Monitor the effectiveness of controls in place to retain integrity, quality and compliance

Role	Responsibility
Information Stewards (including data and content stewards)	<ul style="list-style-type: none"> • Define their information asset • Review and approve security access controls in relation information assets • Communicate and promote the value of their information asset • Monitor and improve conformance with information processes, standards and guidelines • Improve the quality of their information asset • Manage, resolve or escalate information asset related issues
Managers	<ul style="list-style-type: none"> • Ensure employees, contractors and contracted providers understand their information obligations and comply with Ministry information policy, processes, and standards.
All Ministry staff, contractors and contracted providers	<ul style="list-style-type: none"> • Understand the responsibilities that this policy and its associated standards and guidelines place upon them • Manage and use information appropriately by looking after it as an asset, storing and handling it in accordance with Ministry processes and using it with integrity • Create accurate, complete, impartial and accessible records of decisions and actions • Save records in approved Ministry recordkeeping systems, so that they can be easily found and used by others, now and in the future • Create good quality information – accurate, factual, non-defamatory and well-described • Share and reuse information with colleagues at the Ministry of Foreign Affairs and Trade
Data, Content and Information Management Specialists	<ul style="list-style-type: none"> • Support the effective management of information assets at both an enterprise and operational level by implementing this policy in support of business information requirements, applying any legislation or government directive, and adopting and promoting procedures, guidelines and practices, to support organisational information management initiatives

Context

At the Ministry of Foreign Affairs and Trade, information is one of our greatest assets. This policy sets out the various requirements for how the Ministry shall manage and use information to:

- demonstrate transparency and accountability;
- support better operational and policy decisions; and
- unlock the value of our information

Principles

The Ministry will manage its information obligations in accordance with the principle of kaitiakitanga. The Ministry shall demonstrate kaitiakitanga by stewarding its information so that:

- users have trust and confidence in it
- transparency and accountability is demonstrated
- information is managed and used with integrity and manaakitanga – treating it as an Aotearoa New Zealand asset
- the Ministry approach reflects te ao Māori needs and interests in information.

Policy statements

Well-managed

1. The Ministry will manage information well and with integrity throughout its life; and value it as an organisational asset:
 - a. All Ministry staff, contractors and contracted providers will create reliable and trustworthy records as evidence of transactions, decisions and actions.
 - b. Ministry staff will describe information assets to recognised standards.
 - c. The Ministry will provide approved compliant recordkeeping systems and storage locations; and make them secure from unauthorised access, disclosure, alteration, deletion, loss or destruction.
 - d. Ministry staff will store records in those systems and/or locations.
 - e. Access to, use of and sharing of information by Ministry staff must be in line with our legal requirements and obligations, including the New Zealand Official Information Act 1982, Privacy Act 2020, Code of Conduct, Contract and Commercial Law Act 2017, Public Records Act 2005 and the Protective Security Requirements.
 - f. Information will be managed in accordance with international protocols, conventions and obligations.
 - g. Information will be managed by the Ministry through its life-cycle including long-term preservation and access, and catering for technological obsolescence.
 - h. Information will be kept for as long as needed for business, legal and accountability requirements. Staff with appropriate delegations will then systematically dispose of information when authorised and legally appropriate to do so, using a managed process. In the case of information, which must be transferred to Archives New Zealand, the Ministry will declassify then release that information.
 - i. Information identified as being of significant value – whether to inform decision-making or of historical and cultural importance – shall be managed by the Ministry in such a way as to support deriving value from that information.
2. All Ministry projects to develop new systems and/or processes will ensure that information and records management is built into those systems and/or processes.
3. The Ministry will manage its information as a taonga and a historical asset, looking after it on behalf of Aotearoa New Zealand in such a way that its value can be harnessed.
4. Information of interest to Māori will be identified, and management of and access to that information will reflect understood Māori needs and interests.
5. If the Ministry identifies gaps and or risks in the flow of information, it will document them, mandate any required improvements, and report on progress.

Subject to effective governance

6. The Ministry will demonstrate leadership in the governance of information, both within the Ministry, and with that NZ Inc information for which it is the custodian.
7. The Ministry shall maintain executive and operational roles which are accountable for records and information management.
8. The Ministry will ensure that all information assets and products has assigned stewards who proactively manage their assigned Ministry assets.
9. Stewards will be assigned for information created within any functions outsourced by the Ministry, conducted in partnership with the Ministry, and by the Ministry itself.
10. The Ministry will maintain effective information and records management governance frameworks.
11. The Ministry will identify what information is needed by the Ministry in its statutory roles, and the activities which create information to ensure:
 - a. Information is only collected for specific policy, operational business or legislative purposes, and
 - b. Information supports the purposes for which it was collected.

Unlock and use

12. Information will be made available to benefit Aotearoa New Zealand citizens and businesses, iwi, the public sector, counterparts, partners and international institutions and organisations, unless there are reasons to restrict access.
13. Internally, the Ministry will make information open by default unless there is a good reason to restrict access.
14. Ministry staff will be trusted to balance "need to know" with "responsibility to share".
15. The Ministry prefers digital over paper which means we digitise business processes, in line with legal requirements; and will store born-digital information digitally, rather than printing it out and storing it in paper form.
16. The Ministry will enable the fullest appropriate use of our information through:
 - a. better data access and transformation into reports and dashboards to support evidence-based decision making and internal and external reporting
 - b. adoption of the CC-BY Creative Commons license over our published information, which permits others to distribute, remix and build upon Ministry work, even commercially, as long as they credit the Ministry for the original creation
 - c. proactively releasing and opening up our information through publishing high-value information to our website and to data.govt.nz
 - d. use of common data and information metadata schemas, such as JSON, and the data.govt.nz metadata schema
 - e. publishing high-value corporate information such as policies, guides, forms and people information to our intranet
 - f. publicly releasing our high value historical information, and creating or facilitating the creation of new knowledge products off that information
 - g. creating new use and utility from existing information, and

- h. enabling safe internal and external content collaboration.

Exceptions management and consequences of policy breach or non-compliance

Any deviation from this policy must be approved in advance by the appropriate authority as defined in the Instrument of Delegation; and informed to the Ministry Data and Information Governance Group. If this is not specifically defined in the Instrument of Delegation, then the Deputy Secretary of the relevant division where the deviation is to occur must approve any deviation in advance. The deviation must be notified to the policy owner and sponsor, and the Divisional Manager, Audit and Risk.

Unauthorised breaches of this policy may be viewed seriously by the Ministry as a breach of the Code of Conduct. The Code of Conduct states that "employees are expected to fully comply with Ministry policies in their work". Depending on the circumstances, breach of this policy may result in disciplinary action, up to and including dismissal. Any such breaches should be notified to the policy owner and sponsor and the Divisional Manager, Audit and Risk.

Related content

The following Ministry documents are also relevant/related to this policy:

- ICT Acceptable Use Policy
- Privacy Policy
- Risk Management Policy
- <https://protectivesecurity.govt.nz/information-security/>
- Corporate Policy Framework

Relevant legislation and regulations

The Ministry must comply with the following legislation/regulations:

- Public Records Act, 2005
- Contract and Commercial Law Act 2017
- Privacy Act 2020
- Official Information Act 1982
- New Zealand Data and Information Management Principles - data.govt.nz¹
- Declaration on Open and Transparent Government - data.govt.nz²

National standards

The Ministry must comply with the following New Zealand data standards.

- Register of government mandated data standards - data.govt.nz³

Related training

The Ministry provides the following training related to this policy:

¹ <https://www.data.govt.nz/toolkit/policies/new-zealand-data-and-information-management-principles/>

² <https://www.data.govt.nz/toolkit/policies/declaration-on-open-and-transparent-government/>

³ <https://data.govt.nz/toolkit/data-standards/mandated-standards-register/>

- Information management training
- GDM training
- Executive data briefing for managers
- Data and analytics

Annex B - Declassification and release of historical information - Standard

Purpose

This standard outlines how the Ministry for Foreign Affairs and Trade (the Ministry) approaches the review and declassification of high value historical records for public release and Ministry internal use.

The Information Policy must be read in conjunction with this standard.

Context

The Ministry has obligations under the Official Information Act (OIA) 1982⁴, Public Records Act 2005⁵ and the Declaration on Open and Transparent Government 2011⁶ to make official information and data open and accessible.

This standard aims to improve access to information for the purposes of research and reuse, while supporting the Ministry's operational activities and protecting the Ministry's security interests.

This standard contributes to the Ministry's strategic goal to foster New Zealand connections by ensuring that the public has easier access to information about New Zealand's international relations, development and trade policies and activities.

Standard Categories

Review and Declassification of Records (Vetting)

Release of Records

Standards

Review and Declassification of Records (Vetting)

1. The Senior Historical Information and Research Advisor - Declassification should review and where possible declassify historical records dated 25 years or older from the file closure date. Exceptions can be made to the 25 year rule on a case by case basis if the material is considered to be of great historical significance.

4

http://legislation.govt.nz/act/public/1982/0156/latest/DLM64785.html?search=ts_act%40bill%40regulation%40deemedreg_%e2%80%a2%09Official+Information+Act+1982_resel_25_a&p=1

5

http://legislation.govt.nz/act/public/2005/0040/latest/DLM345529.html?search=ts_act%40bill%40regulation%40deemedreg_%e2%80%a2%09Public+Records+Act+2005_resel_25_a&p=1

⁶ <https://www.data.govt.nz/manage-data/policies/declaration-on-open-and-transparent-government>

Review and Declassification of Records (Vetting)

2. The Senior Historical Information and Research Advisor - Declassification should give priority for review, records determined as high value to:

- New Zealand's foreign policy and trade history.
- Domestic stakeholders such as Māori, the business sector, civil society, Pasifika and Asian communities and academia.
- Academic or bona-fide researchers upon application to the Ministry.
- The Ministry upon internal recommendations.

3. The Senior Historical Information and Research Advisor - Declassification must approach each record with the assumption of openness unless there is a good reason to restrict the record. This approach is in accordance with Archives New Zealand's Access 16/G06 document⁷, Public Records Act section 44⁸, and the Official Information Act Standard.

4. The Senior Historical Information and Research Advisor - Declassification must place access restrictions on records in order to protect national security, economic stability, international relations and/or individual privacy. These decisions will be made following the Ministry's Vetting Guidance the Ministry's internal Security and Privacy policies and the Official Information Act⁹. Decisions on these restrictions may be made in consultation with the wider Ministry.

5. The Senior Historical Information and Research Advisor - Declassification must record all decisions on a Classification Review Sheets and complete a file release statement to be placed on each record.

Rationale:

Under Sections 43 and 44 of the Public Records Act 2005¹⁰ all Ministry Records transferred to Archives New Zealand are required to be classified as either Open Access or Restricted Access. For Restricted Records, access conditions must clearly state the reasons for the restriction, expiry or review date, and any use conditions.

Release of Records

1. Historical records held at Archives New Zealand that have been identified as releasable by Senior Historical Information and Research Advisor - Declassification must be considered for release through the process: Manage release of files.

2. Historical records held with the Ministry must first be transferred to Archives New Zealand before they can be included in the process: Manage release of files.

⁷ <https://records.archives.govt.nz/resources-and-guides/access/>

⁸ <http://www.legislation.govt.nz/act/public/2005/0040/latest/DLM345772.html>

⁹

¹⁰ http://legislation.govt.nz/act/public/1982/0156/latest/DLM64785.html?search=ts_act%40bill%40regulation%40deemedreg_%e2%80%a2%09Official+Information+Act+1982_resel_25_a&p=1

http://legislation.govt.nz/act/public/2005/0040/latest/DLM345529.html?search=ts_act%40bill%40regulation%40deemedreg_%e2%80%a2%09Public+Records+Act+2005_resel_25_a&p=1

3. The Ministry must meet its obligations outlined in the Memorandum of Understanding between the Ministry and Archives New Zealand. This includes giving Archives New Zealand advance notice prior to the Ministry's monthly and thematic release of historical records through the process: Manage release of files.

Rationale:

Under Sections 43 and 44 of the Public Records Act 2005, if there are no good reasons to restrict records, the restriction must be changed to open access (released).

Application

This standard will apply to all Ministry employees and contractors.

These standards apply to all Ministry records, including records transferred to Archives New Zealand or held internally, regardless of format.

Detailed Roles and Responsibilities

The following roles have specific responsibilities under this standard:

Role	Responsibilities
DCE People and Operations	Final sign off on release process
Chief Information Security Officer	Consults on management of information security
Privacy Officer	Consults on information privacy
Senior Historical Information and Research Advisors - Declassification	<ul style="list-style-type: none"> • Reviewing and declassify records as per instrument of delegation • Connecting with internal stakeholders • Identifying records of high value
Manager, Historical Information and Research Team	<ul style="list-style-type: none"> • Managing requests from researchers • Connecting with key internal and external stakeholders • Identifying records of high value • Leading release process

Exceptions management and consequences of standard breach or non-compliance

This standard is mandatory and must be complied with. For details on exceptions management, please refer to Information Policy.

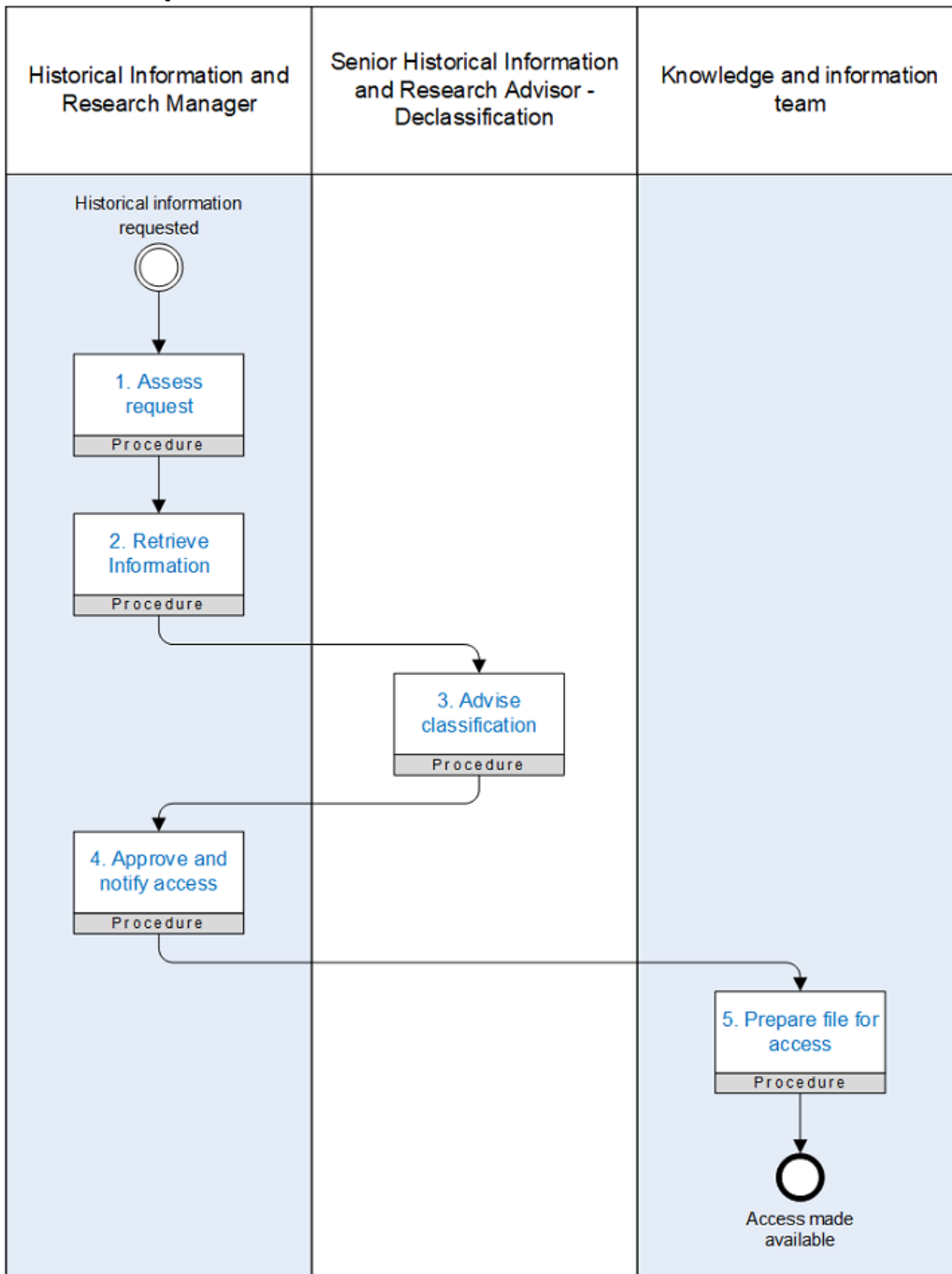
Exceptions can be made to the 25 year rule on a case by case basis if the material is considered to be of great historical significance.

Annex C - Managing access requests for historical classified information - process

Purpose

The purpose of this process is to explain how to handle an external request to access historical Ministry information (over 25 years) that is still classified. This process covers the identification of relevant information, an assessment of the access that can be offered, and a preparation of the files for access.

Process map



Annex D - 2022-2023 PSR Self-Assessment Report

Plan for adoption of the updated Classification System Policy

What changes are required within the organisation to adopt the updated policy?

In the main the Ministry has already implemented many of the aspects the updated policy seeks to achieve. We will need to ensure the new principles are well understood across the organisation. This will be an ongoing piece of work coordinated by the CSO, CISO and security staff.

Further tools and training are required to help staff more accurately classify material. The Ministry intends to utilise the training material provided on the PSR website for our internal awareness raising programme.

What will the agency do over the next 12 months? Future years?

The Ministry will seek to maintain the levels where it has achieved compliance, as it applies to the classification system. We are anticipating further staff changes and will need to manage this closely.

We are addressing the changes made in updating the Classification System. We have accommodated the changes in our training and awareness program in an informal manner, but more broadly we plan to update our documentation. Those changes will then be adopted by the wider organisation.

Annex E - 2023-2024 PSR Self-Assessment Report

Implementation of the updated Classification System Policy

Are your internal policies and procedures updated to reflect the 2022 changes in the Classification System policy?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> In Progress	<input type="checkbox"/> No
What date have you planned for full implementation?	Not applicable		
Have you adopted the Classification training modules for your agency or incorporated the refreshed guidance into your existing security training programme?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No	
Do you have a Declassification programme?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> In Progress	<input type="checkbox"/> No

Please outline what your agency's next steps are for embedding the Classification System policy:

The Ministry intend to integrate the five PSR Classification training modules into the Ministry's protective security training.