RENEWABLE HEAT INCENTIVE INQUIRY

RHI Inquiry
1st Floor, Waterfront Plaza
8 Laganbank Road
BELFAST BT1 3LY

T: 028 9040 8833
E: general@rhiinquiry.org
W: www.rhiinquiry.org

Damian Martin
Head of IT Assist
Enterprise Shared Services
Craigantlet Buildings
Stoney Road
Belfast
BT4 3SX

By post and email: (Damian.Martin@Finance-ni.gov.uk)

31 May 2018

Dear Damian

Re: The Independent Public Inquiry into the Non Domestic Renewable Heat Incentive (RHI) Scheme
Provision of a Section 21 Notice requiring the provision of evidence in the form of a written statement

I refer to the assistance provided to the Inquiry by ESS in relation to the retrieval of evidence from NICS email accounts and NICS mobile telecommunication devices to which witnesses to the Inquiry no longer had access. I once again wish to thank you and your team for their hard work in this matter.

You have previously provided the Inquiry with two witness statements, on foot of Notices 250 of 2017 and 323 of 2017 respectively, which deal with the retrieval, and provision to the Inquiry, by ESS of evidence in relation to NICS owned mobile telecommunication devices issued to certain persons.

The purpose of the attached section 21 Notice is to obtain a further statement from you in order to detail the work carried out by ESS in the retrieval, and provision to the Inquiry, of evidence from specified NICS email accounts.

As discussed, for completeness the Inquiry requires a further statement providing some additional detail in relation to the work ESS has conducted to date; and also providing further information in respect of some of the telephone devices identified by you in your first statement. For these purposes, please find attached a further section 21 Notice requiring the provision of same. (As before, the legal requirement for you to provide this material to the Inquiry pursuant to its statutory powers should allay any concerns you might otherwise have had in relation to, for instance, confidentiality).

Please do not hesitate to contact me to discuss any matter arising.

Yours faithfully

Patrick Butler
Solicitor to the RHI Inquiry
02890408928

SCHEDULE

[No 107 of 2018]

1. Please provide any and all policies issued by the Northern Ireland Civil Service ("NICS") in relation to the creation, deletion, use/misuse of NICS email accounts during the period January 2011 to March 2017.

2. Please outline the policy, if any, for the creation of NICS email accounts upon the appointment of a new Minister or Special Adviser within a Northern Ireland government department.

3. In respect to each of the following persons:

    (a) Jonathan Bell
    (b) Timothy Cairns
    (c) Andrew Crawford
    (d) Arlene Foster
    (e) Timothy Johnston
    (f) John Robinson

    provide details of the Northern Ireland Civil Service ("NICS") email accounts created, or in existence, for each of them to use during the period January 2011 to March 2017 while they were appointed Minister or Special Adviser, as the case may be.

4. Please detail the process(es) or mechanism(s) used by ESS to identify each of the NICS email accounts identified in response to question 3 above.

5. Please detail any and all relevant procedures and mechanisms by which the Northern Ireland Civil Service ("NICS") routinely created 'backed-up' copies, or otherwise saved or archived, NICS email accounts during the period January 2011 to March 2017; and explain the process by which such back-up copies, saved accounts or archived accounts are now accessible by ESS.

6. Where no such back-up, saved or archived copies exist for any period of time during October 2011 to March 2017 please detail the reason(s).

7. The Inquiry requested that ESS provide it with back-up, saved or archived copies of any NICS email accounts for the following persons for specified periods during November 2015 to March 2017, namely:

   (a) Jonathan Bell
   (b) Timothy Cairns
   (c) Andrew Crawford
   (d) Arlene Foster
   (e) Timothy Johnston
   (f) John Robinson

   Please explain the procedures and processes ESS undertook to retrieve and provide this evidence to the Inquiry. Where ESS was unable to retrieve any or all of an email account requested, or for any or all of the period requested, please detail the reason(s) why and any further actions taken by ESS in an attempt to retrieve the information.

8. Please detail the email accounts and time periods in respect of which ESS retrieved and provided email material to the Inquiry.

9. Please explain the format in which the retrieved email accounts were provided to the Inquiry; the process(es) or mechanism(s) by which the email accounts can be viewed by the Inquiry; and any mechanism(s) by which they searched by the Inquiry.

10. In the email accounts retrieved by ESS and provided to the Inquiry, please explain the difference between those folders named "Deleted Items" and those folders named "Deletions".

11. In the email accounts retrieved by ESS and provided to the Inquiry, please explain why ESS was unable to retrieve a back-up copy of any email account for 'December 2015'; and please detail the period(s) of time in or around December 2015 when no back-up copies of NICS email accounts are available to ESS.

12. Please provide any further information you consider of relevance in understanding the assistance provided by ESS to the Inquiry and/or the limitations available upon the email material which the Inquiry was able to consider as a result of its engagement with ESS.

13. Please provide any further information you consider relevant to the work of the Inquiry having regard to its Terms of Reference.

RENEWABLE HEAT INCENTIVE INQUIRY

INQUIRY INTO THE RENEWABLE HEAT INCENTIVE SCHEME

RHI REF: Notice 107 of 2018

DATE: 13th June 2018

Witness Statement of: Damian Martin

I, **Damian Martin**, will say as follows: -

1. **Please provide any and all policies issued by the Northern Ireland Civil Service (NICS) in relation to the creation, deletion use/misuse of NICS email accounts during the period January 2011 to March 2017.**

Three policy documents have been issued by Department of Finance referring to email usage, as follows;

a. HR Handbook, Section 6.01 Standards of Conduct – Annex 9, Internet and Email Usage, available via HR Connect portal (attachment A – HRHandbookAx9).
b. DoF Records Management Handbook, Section 5, Creating and Capturing Records, available on NICS Intranet (attachment B – RMHandbookS5).
c. DoF Records Management Policy 2016 – 2019, available on NICS Intranet (attachment C – RMPolicy).

2. **Please outline the policy, if any, for the creation of NICS email accounts upon the appointment of a new Minister or Special Adviser within a NI government department.**

There is no written policy for the creation of NICS email accounts. The process used, following receipt of a Service Request, to create email accounts for

Ministers and Special Advisors was that Enterprise Shared Services would create generic Departmental Minister and Special Advisor email accounts (eg. Minister_DoF and SPAD_DoF). While there would only be one email account for a Minister and a SPAD, there is an option, if requested, to add multiple and varying email addresses to that email account. Accordingly the generic email account can send and receive email using multiple email addresses. Who the email account holder granted authority to access the email account is an entirely separate matter. An example would be emails sent to and from "Minister_DoF@finance-ni.eu" and "Minister_DoF@dfpni.gov.uk" et cetera would be accessed from the one email account. This process was not, however, always followed because in some cases Ministers and Special Advisors specifically requested an individual email account, as opposed to a generic email account, and an individual email address. Accordingly, Timothy Cairns requested an individual email account, (eg. CairnsT), and an individual email address, (eg timothy.cairns@detini.gov.uk). This resulted in the generic email Account and Mailbox being disabled and not used.

3. **In respect to each of the following persons provide details of the NICS email accounts created, or in existence, for each of them to use during the period January 2011 to March 2017 while they were appointed Minister or Special Adviser as the case may be:**

While some of the following Email Accounts would have existed prior to November 2015, it is not possible to restore emails for the period January 2011 to October 2015 as tape backups no longer exist. The following is a list of the Email Accounts and primary Email Addresses used by the named persons for the period November 2015 to March 2017;

(a) **Jonathan Bell**

ESS were unable to identify an NICS email account used by Jonathan Bell for the period in question.

(b) **Timothy Cairns**

Mailbox = CairnsT (timothy.cairns@detini.gov.uk)

(c) **Andrew Crawford**

Mailbox = Crawforda (andrew.crawford@detini.gov.uk)

(d) **Arlene Foster**

Mailbox = Fostera (arlene.foster@detini.gov.uk)

(e) **Timothy Johnston**

Mailbox = JohnstonT (timothy.johnston@ofmdfmni.gov.uk)

(f) **John Robinson**

Mailbox = DFE SPAD (spad@economy-ni.gov.uk)

It appears that in respect of those persons set out at (a) to (f) above, only John Robinson had a generic email account with a single email address, the persons at (a) to (e) all had an individual email account with an individual email address.

4. **Please detail the process(es) or mechanism(s) used by ESS to identify each of the NICS email accounts identified in response to question 3 above.**

The process used to identify the email accounts used by the named persons involved two steps. Firstly, a search was carried out of Service Requests submitted to ESS asking for new email accounts to be created for the named individuals and the terms "Minister" and "SPAD", which provided an approximate timeframe for when the email account was created. Secondly, the timeframe for account creation was then used to review Active Directory backups to determine the mailbox name used when the email account was created.

5. **Please detail any and all relevant procedures and mechanisms by which the NICS routinely created 'backed-up' copies, or otherwise saved or archived, NICS email accounts during the period January 2011 to March 2017; and explain the process by which such back-up copies, saved accounts or archived accounts are now accessible by ESS.**

ESS maintain tape backups of all systems provided to the NICS. These tapes are typically retained for a 12-month period and then overwritten. The primary purpose of these tape backups is to allow data to be restored in the event of a

system failure or loss of data. Tape backups of the NICS email system are, however, held from November 2015, (the reason for this is explained in paragraph 6 below). The tape backups held from November 2015 to March 2017 are monthly snapshots of the NICS email system taken at the start of each month and contain a full copy of all email that existed at the time the backup/snapshot was taken. The main limitation of this approach was the tape backups only held copies of the mailboxes and messages that existed at the time the snapshot was taken. When the next monthly snapshot was taken it would not have included any messages sent or received during the preceding month if they had been deleted by the user before the next snapshot was taken. Much, therefore, depended on the practise of the user. From April 2017, however, this process was updated and the backups/snapshots held by ESS from that time are taken daily.

These tape backups can be restored to create a copy of the email system that existed at the time the tape backup was taken.

6. **Where no such back-up, saved or archived copies exist for any period of time during October 2011 to March 2017 please detail the reason(s).**

Tape backups of the email system prior to November 2015 do not exist. As mentioned in response to paragraph 5, ESS typically maintain 12 months of tape backups for use in emergency situations, where there is a system failure or loss of data. The email system tape backups exist back to November 2015, however, because in late 2016, IT Assist were planning for a major upgrade to the email system and for that reason a decision was taken that overwriting tape backups should be postponed in anticipation that issues/difficulties arose with data availability following the upgrade. At that time the earliest available tape backup of the email system was November 2015, and that remains the case. There are no other backups or archives for the email system.

7. **The Inquiry requested that ESS provide it with back-up, saved or archived copies of any NICS email accounts for the following persons for specified periods during November 2015 to March 2017, namely:**

(a) Jonathan Bell
(b) Timothy Cairns
(c) Andrew Crawford
(d) Arlene Foster
(e) Timothy Johnston
(f) John Robinson

Please explain the procedures and processes ESS undertook to retrieve and provide this evidence to the Inquiry. Where ESS was unable to retrieve any or all of an email account requested, or for any or all of the period requested, please detail the reason(s) why and further actions taken by ESS in an attempt to retrieve the information.

The procedures and processes used by ESS to retrieve and provide the requested evidence to the Inquiry involved two stages: One, to recover the database containing the mailbox/email account to be restored from the tape backup; and two, recover the mailbox/email account for the person identified from the database.

Recover the required database from tape backup

1. Identify which database the mailbox was residing in for each of the month(s) during the time period specified for a named person.
2. Identify the location of the tape(s) containing the mail database holding the mailbox to be restored.
3. Retrieve the tape(s) from either the Data Centre Tape Library or Offsite storage location.
4. Restore the required database to a specified folder on one of the ESS dedicated email Servers.

Recover the mailbox from the recovered database

1. Mount the required database, to allow mailboxes to be retrieved.
2. Confirm the mailbox exists in the recovered database.
3. Extract the requested mailbox to a Personal Storage file (PST).
4. Confirm that all held data had been restored, by checking number of items (messages and folders) restored against the database contents.

5. Save the restored PST file and name it according to the person and month of the restore.
6. Encrypt PST file and copy to a PC as directed by the Inquiry.
7. Unencrypt PST file once transferred to the Inquiry, and attach to the Inquiry members Outlook for access.

ESS retrieved all email messages, for the period November 2015 to March 2017, held for the named persons set out at paragraph 7 with the exception of Jonathan Bell, where no email account information was found. ESS followed this up with DETI who were unable to identify an NICS DETI email account used by the then Minister, Jonathan Bell.

As previously mentioned, ESS hold tape backups for the period November 2015 to date. It is, however, important to distinguish the fact that emails earlier than November 2015 may be available from those November 2015 backup tapes, if retained by the user in accordance with the "3-month Retention rule" (an automated records management policy that deletes messages older than 90 days). Accordingly some of the November 2015 backup/snapshot would also have held email messages going back a previous 3 months, (ie August 2015), unless these had been specifically deleted by the user before the monthly backup/snapshot was taken. Again much depended on the practise of the user.

8. **Please detail the email accounts and time periods in respect of which ESS retrieved and provided email material to the Inquiry.**

The email accounts and time periods retrieved by ESS, and provided to the Inquiry, were as follows;

Timothy Cairns:	November 2015 to September 2016 (timothy.cairns@detini.gov.uk).
Andrew Crawford:	November 2015 to June 2016 (andrew.crawford@detini.gov.uk).
Arlene Foster:	November 2015 to May 2016. (arlene.foster@detini.gov.uk)

Timothy Johnston: November 2015 to March 2017
(timothy.johnston@ofmdfmni.gov.uk)
John Robinson: June 2016 to February 2017
(spad@economy-ni.gov.uk)

The December 2015 monthly backup/snapshot failed to complete as it was wrongly configured, and for this reason no snapshot for December 2015 exists. However, under the 3-month Retention rule, (set out at paragraph 7 above), the snapshot taken in January 2016 would have included any messages in the mailboxes for the previous 3 months, unless of course these had been specifically deleted by the user involved.

9. **Please explain the format in which the retrieved email accounts were provided to the Inquiry; the process(es) or mechanism(s) by which the email accounts can be viewed by the Inquiry; and any mechanism(s) by which they [sic] searched by the inquiry.**

The retrieved email accounts were provided to the Inquiry in Personal Storage File (PST) format. This meant that the retrieved email accounts could be provided to the Inquiry team as local copies of the mailbox, including all of its sub-folders, and attached to the Inquiry Team's Outlook email program. These mailboxes could then be viewed and searched, by the Inquiry Team, using Outlook's own search engine, in the same way the Inquiry Team could view and search their own individual email accounts.

10. **In the email accounts retrieved by ESS and provided to the Inquiry, please explain the difference between those folders named "Deleted Items" and those folders named "Deletions".**

Deleted Items is a default email folder which holds all emails that have been specifically deleted by the user. Users can retrieve deleted messages from this folder without the need of an email restore. Messages in this folder are removed under the 3 Month Retention rule, or by the user selecting Empty Deleted Items.

Deletions is a system folder where messages deleted from the Deleted Items folder (as outlined above) are moved to and held on the server as an additional quick recovery method, without a mailbox restore having to be carried out. Messages in this folder are held for 14 days and then deleted by the system.

11. **In the email accounts retrieved by ESS and provided to the inquiry, please explain why ESS was unable to retrieve a back-up copy of any email account for December 2015; and please detail the period(s) of time in or around December 2015 when no back-up copies of NICS email accounts are available to ESS.**

ESS were unable to retrieve email accounts from the December 2015 backup, as that backup failed due to it being configured incorrectly. However, under the 3-month Retention rule for emails, the snapshot taken in January 2016 would have included any messages in the mailboxes for the previous 3 months unless these had been specifically deleted by the user involved.

12. **Please provide any further information you consider of relevance in understanding the assistance provided by ESS to the Inquiry and/or the limitations available upon the email material which the Inquiry was able to consider as a result of its engagement with ESS.**

Before the change in April 2017, (see paragraph 5), the tape backups contained snapshots of the mail system at a point in time. These snapshots were basically a full copy of every mailbox that existed on the system when the snapshot was taken. Individual mailboxes restored from the snapshot would contain all email sent and received during the previous 3 months, unless they had been specifically deleted by the user before the snapshot was taken.

This is why it was possible to retrieve email messages going back to August 2015 even though the earliest tape backup available was taken in November 2015.

RENEWABLE HEAT INCENTIVE INQUIRY

13. **Please provide any further information you consider relevant to the work of the Inquiry having regard to its terms of reference.**

Nothing further to add.

Statement of Truth

I believe that the facts stated in this 9 page witness statement to be true.

Signed: Damian Martin

Dated: 13th June 2018

6.01 Standards of Conduct

ANNEX 9

Internet and Email Usage

1 Introduction

This Annex sets out the policy and provides guidance on the use of the internet and e-mail by Civil Servants. Internet and e-mail facilities can deliver significant business benefits and advantages when used appropriately and responsibly. However, careless or negligent use may waste resources and cause financial loss and damage to reputation. Also, misuse can lead to complaints or legal proceedings against NICS departments or individual members of staff. The rules are intended to protect the interests of the NICS, as well as the interests of users, and to ensure that individuals are not at risk of disciplinary action, criminal proceedings or civil action as a result of misunderstanding or a lack of guidance. The general principles and rules on such usage covering the staff in the Northern Ireland Civil Service (NICS) are set out below.

2. Principles

2.1 Many NICS staff use internet and e-mail facilities on departmental/agency Information and Communications Technology (ICT) resources on a daily basis. The rules in this Annex cover all such staff and, additionally, others given permission to use these facilities. These rules extend to the use of all other NICS ICT resources, where relevant. The rules also apply to the use of non-NICS equipment or facilities (including personal IT equipment at home or elsewhere) for the discharge of official business, for example, for work-related research or working from home. Any Civil Servant working under a homeworking arrangement who has NICS equipment installed in their home for official use will also be subject to the rules. The precise application of general principles of usage will vary with the circumstances of different Departments and may call for special rules for particular staff. Such rules are normally drawn up after consultation with the Trade Union Sides of the Central Whitley Council and the representatives of the Industrial Trades Unions. Disciplinary action against individual members of staff is the responsibility of employing Departments. The following general principles apply to all members of the NICS:

a. individuals must not use non-NICS equipment or facilities for official business unless they have prior permission to do so;

b. if such permission is granted they must ensure that such use does not compromise the security of official data or expose NICS systems or equipment to the risk of disruption from any source, such as a virus attack or unauthorised access;

c. staff should seek advice, when necessary, about IT security matters via their usual departmental/agency IT contacts;

d. staff who use, or intend to use, NICS internet or e-mail facilities for any purpose are required to acknowledge, either in writing or electronically at log-in/sign-on, that they have read, understood and will adhere to, the NICS policy and any related departmental or agency policies;

e. such undertakings should be renewed if the Internet and e-mail usage policies change;

f. failure to comply with the requirements of the NICS policy, and all other relevant departmental/agency policies, may result in disciplinary action – including dismissal; and

g. staff should be aware that e-mails are regarded as a form of publication and are discoverable as part of the

official record.

3. Monitoring and Privacy

3.1 Staff should note that, as is permitted by legislation, NICS Departments will monitor and review Internet and e-mail activity, analyse usage patterns and may publish resultant data (traffic monitoring [1]).

3.2 Departments will also monitor the content of e-mails, files and the like as and when this is considered necessary in order to ensure the integrity of NICS systems and that users are complying with all the relevant usage policies and guidance (content monitoring [2]). Any attempt to disrupt Departmental monitoring amounts to misconduct and may result in disciplinary action.

3.3 Use will be routinely monitored from time to time, and may be specifically monitored at any time when this is deemed necessary for compliance or other reasons, including the prevention or detection of illegal activities.

3.4 Users of NICS ICT resources, including Internet and e-mail facilities, should be aware, and must accept as a condition of use, that their usage of such facilities might be monitored and should have no expectation of privacy whether use is for the conduct of official business or for personal use.

3.5 Departments reserve the right to inspect and examine any and all IT equipment (including personally owned equipment) used on or off official premises, used for the conduct of official business, or connected in any way to the NICS Network, in order to ensure compliance with NICS, departmental/agency Internet or e-mail usage policies. Therefore, users should clearly understand that if they bring into the workplace personal IT equipment of any nature, including laptop computers, or any other electronic or telecommunication device, any such equipment or ancillaries, and data held thereon, may be inspected at any time to ensure that they do not pose a risk to the NICS whether by way of virus infection, hacking software or the presence of improper, offensive or illegal material.

4. Access to Facilities

4.1 Departments may make Internet and e-mail facilities and other ICT resources available o staff for use in carrying out official duties. Access to the internet and e-mail may be made available to staff from desktop PCs. Access to the internet may also be made available to staff through shared Departmental facilities in libraries, resource centres etc.

4.2 Departments may prevent connection of certain machines (holding sensitive data or applications) to the Internet or restrict use of Internet features such as file transfers, and will bar access to sites identified as containing inappropriate material.

4.3 Departments are responsible for the issue of User IDs and/or passwords to maintain individual accountability for Internet and e-mail usage. Individuals will be held responsible for the security of IDs and passwords and, where appropriate, for the return of passcards on leaving a Department’s employment.

4.4 Departments are responsible for ensuring that facilities provided for Internet and e-mail access meet all relevant health and safety legislation.

4.5 Users must respect the privacy and legitimate rights of others, just as would be appropriate in any other work activity.

4.6 Individuals will be held accountable for any misuse or breach of security, including confidentiality. Such misuse may lead to disciplinary action.

4.7 Where circumstances dictate, Departments will inform and co-operate with relevant legal enforcement bodies.

4.8 Access to Internet and e-mail facilities may be withdrawn at any time as a result of, or pending the outcome of, investigations into suspected misuse.

5. General Responsibilities of Users

5.1 All the usual NICS rules relating to conduct and normal standards of behaviour apply just as much when using ICT facilities as at other times.

5.2 Users must at all times conduct themselves responsibly and honestly when accessing the Internet or when using e-mail facilities.

5.3 Individuals must ensure that their actions do not:

a. waste time or resources;

b. expose the NICS Network, or data held thereon, to the risk of corruption, loss or inadvertent disclosure;

c. cause offence to colleagues or others;

d. breach any law or statute; or

e. otherwise bring the NICS into disrepute.

5.4 Unacceptable behaviour is just as serious an offence if made in the course of using ICT facilities as at any other time. Examples include:

a. harassment or bullying;

b. dissemination or display, for example, as a screen saver, of inappropriate material (see 4.5 below);

c. offensive remarks or comments of a sexual, racial or sectarian nature; or

d. offensive remarks or comments regarding sexual orientation, religious belief, political opinion, marital status, age, disability or dependents.

5.5 Inappropriate material may include, but is not limited to, any material of a pornographic, sexist, racist, sectarian, violent or offensive nature; whether in pictures, cartoons, words, sounds or moving images, whether or not purporting to be of a humorous nature. Staff should be aware that the decision as to what material is considered offensive can depend on the perception of the recipient and/or observer, rather than the intention of the sender.

5.6 Users should be aware that they might be personally liable to prosecution, and open to claims for damages, should their actions be found to be in breach of the law. In cases of harassment, a claim by a user that he/she had not intended to harass or cause offence will not in itself constitute an acceptable defence.

5.7 Users should be aware that the possession of child pornography is a criminal offence. The NICS will fully co-operate with law enforcement authorities to identify and take action against any member of the NICS accessing, possessing or disseminating such material. Individuals found to have been involved in any way in access to or possession or dissemination of child pornography using NICS ICT systems will face serious disciplinary action with a high probability of dismissal irrespective of whether or not they are prosecuted or convicted under the criminal law.

5.8 Within this overall context users may (subject to the safeguards and conditions set out in this and any other relevant policy or guidance):

a. use e-mail to communicate with colleagues, customers, suppliers and other interested parties in carrying out their Civil Service duties;

b. use the Internet to research relevant and potentially relevant information resources in carrying out their duties. In doing so, users may glean relevant information from trusted third parties (including news sites), provided prior approval for such access has been granted by local management; and

c. participate (subject to local management approval) in officially sanctioned newsgroups or chat rooms in the course of business relevant to their duties. When so doing, users must not (unless specifically authorised to do so) speak or write in any department/agency's name and must make it clear that their participation is as an individual speaking only for themselves. In any such use of Internet/e-mail facilities, users must identify themselves, with their own full name, honestly, accurately and completely. When participating in a chat forum or newsgroup users must:

i. refrain from political advocacy and from the unauthorised endorsement or appearance of endorsement of any commercial product or service;

i. give due regard to maintaining the clarity, consistency and integrity of the NICS, departmental/agency corporate image and avoid making any inferences that may prove inappropriate from a departmental/agency or NICS perspective;

and must not:

iii. reveal protectively marked information, customer data, or any other material covered by departmental/agency policies and procedures; and,

iv. use departmental/agency Internet facilities or computing resources to violate applicable laws and regulations in any way or to compromise the security (including confidentiality) of departmental/agency data.

6. Essential Actions for Users

6.1 At all times users must:

a. keep all passwords or user IDs confidential – the sharing of user IDs or passwords is prohibited; any breach must be reported to the IT and Departmental Security Officers;

b. be alert to the risk of leaving an unattended machine logged on, which could lead to unauthorised use of their account and user ID;

c. follow the security procedures approved for use with their system to ensure that any file downloaded from the Internet is scanned for viruses before it is accessed or run. Users who download such files, or who open attachments to e-mails, are responsible for ensuring that they are subjected to appropriate anti-virus scans (checking with the departmental/agency IT Security Officer as necessary);

d. report immediately any indication of virus or other attack to ISU;

e. report immediately to their line manager or, if appropriate, to the departmental/agency Head of Personnel, the receipt of inappropriate or offensive material delivered via e-mail;

f. respect copyrights, software licensing rules and property rights, download only software with direct business use and do so in accordance with relevant departmental/agency policy; and

g. as far as possible, schedule communication-intensive operations such as large file transfers, video downloads, mass e-mailings, etc. for off-peak times.

7. Prohibited User Actions

7.1 Users must not:

a. arrange to auto-forward e-mails from their departmental/agency account to personal e-mail accounts, or from their personal e-mail account to departmental/agency accounts. E-mails received into a departmental/agency

account may be forwarded once their contents have been vetted to ensure that the forwarding of the e-mails does not contravene guidance in respect of protectively marked material;

b. propagate any virus or programme designed to infiltrate a system (without the user's knowledge) to gather information (e.g. worm, Trojan horse) or other type of malicious program code;

c. use any departmental/agency facilities to disable, overload, or gain unauthorised access to any computer system or network, or attempt to disable, defeat or circumvent firewalls or any departmental/agency ICT security facility intended to protect the privacy or security of systems, networks or users;

d. forward, send or store e-mails or other files containing inappropriate material;

e. knowingly connect to any Internet site that contains inappropriate material. When such a site is inadvertently accessed, users will immediately disconnect from the site, regardless of whether that site had been previously deemed acceptable by any screening or rating program. Such inadvertent connections must be reported immediately to the relevant departmental/agency Help Desk so that appropriate action to bar access to the site can be taken and to safeguard the individual in the event of any subsequent investigation;

f. use any departmental/agency systems or facilities to commit infractions such as harassment, unauthorised public speaking, misappropriation of intellectual property or misuse of departmental/agency assets or resources;

g. intentionally access, archive, store, distribute, edit, record or reproduce (on screen, hardcopy or via audio) any kind of inappropriate material (see 4.5 above) on any departmental/agency system;

h. use departmental/agency facilities to download and/or forward non-business related software or data including music, graphics, videos, text, games, screensavers, wallpapers, entertainment or pirated software;

i. use departmental/agency facilities to play Internet games, forward chain letters, or enter on-line competitions;

j. use departmental/agency facilities to participate in chat rooms, forums or newsgroups unless this is for business purposes and has been approved by line management;

k. upload any software licensed to a department/agency or data owned by a department/agency without the express authorisation of the manager responsible for the software or data;

l. transfer via the Internet (as opposed to the NICS Intranet) files containing RESTRICTED departmental/agency data unless the data is first encrypted using a product approved by the appropriate departmental/agency IT Security Officer. Files containing RESTRICTED material may be transferred via NICS Intranet. However, files containing departmental/agency data with a protective marking higher than RESTRICTED must NOT be transferred electronically (except where different departmental rules apply)

m. remain connected to the Internet while not actively using the resource.
n. use departmental/agency internet facilities to undertake unauthorised trading at work, whether buying or selling, through sites such as (but not limited to) e-bay. This amounts to misconduct and may be subject to disciplinary action. Trading is defined as any activity, buying or selling, connected with a commercial or business interest.

8. Other Roles and Responsibilities

8.1 Central Personnel Group (CPG) has responsibility for setting the policy through the usual consultation with Trade Union Side and other stakeholder interests.

8.2 Departmental Personnel Divisions have ownership and responsibility for the overall application of the policy within their Department. Personnel Divisions are also responsible for initiating action following any preliminary

investigation of misuse as part of the disciplinary process and for any subsequent disciplinary action and imposition of penalties.

8.3 Heads of Division and Heads of Branches are responsible for the overall implementation of the policy within their area of responsibility.

8.4. Line managers have the responsibility to ensure that their staff meet their objectives and do not waste business time and/or resources. They are therefore in the best position to ensure that their staff comply with the Internet and E-Mail Usage policy by regularly monitoring their output and observing their behaviour. It is the line manager's specific responsibility to:

• Ensure that their staff are familiar with Internet and E-Mail Usage policy and sign any undertaking regarding usage.

• Monitor through normal supervision of work output their staff's usage of the internet and e-mail.

• Initiate action regarding any abuse or misuse of the Internet and E-Mail Usage policy by discussing the matter with the individual concerned.

• Consult with Personnel on any actual or suspected misuse.

8.5. ISUs should provide and maintain monitoring software. All Departments should use the same software, where possible. ISUs are also best placed to carry out monitoring of internet access and e-mail usage and monitor specific accounts on request from Personnel, where there is suspicion of misuse.

8.6. No specific role is envisaged for Information Technology Security Officers (ITSOs) in applying the policy but they should be kept informed of any abuse or misuse where the security of Departmental systems could be in jeopardy.

8.7. No specific role is envisaged for Departmental and Assistant Departmental Security Officers (DSOs/ADSOs) but they may be able to assist with investigations.

9. Disciplinary Action

9.1 Any breach of the NICS Internet and e-mail Usage Policy will be treated as a matter of misconduct and will be dealt with under the normal Disciplinary Procedure. The nature of any penalty should be proportionate to the seriousness of the offence and each individual case should be treated on its merits.

9.2 There will be clear benefits in applying a consistent approach to any such offence both within the NICS as a whole and within individual Departments. When considering the appropriate disciplinary action in each case of misuse Departments should take into account the following factors:

• The nature and circumstances of the offence

• The extent of misuse

• The extent of time wasted

• The nature of material involved

• The grade and experience of the individuals involved

• History of any previous breaches of the policy by the offender

• Whether the misuse involves any unlawful activity

• Action in previous cases of similar offences

• Mitigating factors

• The level of culpability of the offender

• The extent to which the individual has engaged in and commissioned action by others.

9.3 Certain activities are likely to result in dismissal, such as:

a. deliberately accessing, possessing or disseminating pornography or other offensive material, including material that could incite violence or reflect/promote hatred;

b. serious harassment or bullying via e-mail;

c. deliberate propagation of any virus or otherwise interfering with the integrity of NICS systems; or

d. the possession or use of hacking software on official premises.

10. Personal Use of ICT Facilities

10.1 Personal use is defined as any use of Internet or e-mail facilities that does not relate directly to a requirement of the officer's official duties. Thus accessing a site for research purposes, for example researching social security policy or employment law developments, is official use only if such access is necessary as part of the officer's work. Accessing such data for reasons not related directly to a requirement of the officer's work would be classed as personal use of the information.

10.2 Any access or use which is unrelated to official duties, for example, accessing general news sites, travel information, personal banking, sending or receiving personal e-mails and so on, would be classed as personal use.

10.3 Use of official facilities for personal use will be permitted, providing that such use:

• complies with the requirements of Sections 4-6;

• does not compromise the security of official data, result in increased costs or delays or have any negative impact on the NICS Network or on the effective discharge of official business;

• does not result in personal commercial gain.

10.4 Use of official internet and e-mail facilities for personal use will be restricted to an individual's own time during non-working hours at lunch breaks and before and after work.

10.5. The facility for personal use is granted at the discretion of management and may be withdrawn or refused at any time for operational reasons, or if misuse is suspected or detected. It is not necessary for permission to be sought again once it is granted for a particular personal use.

10.6 Users are reminded that all Internet and e-mail use is subject to monitoring. Such monitoring does not differentiate between official and personal use. Users should therefore ensure that anyone who may send personal e-mails, or other material, to their official e-mail address is aware that the content of such e-mails may be monitored. Use of the NICS facilities for personal use will be deemed as acceptance that usage, and content, will be monitored.

10.7 Subject to departmental/agency policies in relation to personal use, users may in their own time:

a. use Internet access for personal research;

b. use the Internet for the occasional purchase of goods and services, for example, books, flights, CDs, and so on, provided payment is made by the individual, and delivery of items purchased is to a private address. This excludes trading as defined in paragraph 1.20, Private Trading, in the Conduct Section. The user must not create any contractual liability on the part of the NICS. The NICS does not accept any responsibility for the security of credit card details, or any other payment method used. Nor does the NICS accept any liability for financial loss, whether as a result of fraud or otherwise, suffered while using NICS systems for personal transactions. All such use is entirely at the individual's own risk;

c. make occasional use of departmental/agency facilities for on-line banking. All such use will be at the individual's own risk – Departments cannot accept any liability for losses or for any other liabilities arising out of such transactions, howsoever caused; and,

d. make occasional use of departmental/agency e-mail accounts set up on their behalf, to send, forward or receive personal e-mails – subject to the conditions for using e-mail facilities set out above (paragraph 4.8) e-mails must be clearly marked as such. It is an explicit condition of using this facility that users accept that the content of such e-mails may be accessed, by management and/or IT staff, without notice or any requirement for further consent. While it is not intended to undertake routine monitoring of the contents of e-mails (personal or otherwise), e-mail traffic may be accessed at any time either as a result of checking an officer's e-mail account for business reasons if they are absent from work, or as part of an exercise to monitor compliance with Internet and e-mail usage policy.

10.8 Users must not make excessive use of any of the above facilities to the detriment of their official duties.

10.9 Users must not:

a. use departmental/agency Internet or e-mail facilities to carry out any activities for personal gain including, for example, share dealing or monitoring, investment portfolio management, trading, gambling or entering on-line competitions; or

b. set up a personal e-mail account using departmental/agency resources unless prior approval to do so has been given by the Head of ISU; or

c. knowingly connect to any Internet site that contains inappropriate material as defined at paragraph 4.5.

11. Copyright and Similar Issues

11.1 Departments will, where it is deemed appropriate:-

a. retain the copyright to any departmental/agency material posted on any forum, newsgroup, chat room or World Wide Web page by users in the course of their duties; and,

assume ownership of any legitimate software or files downloaded via the Internet on to departmental/agency networks. Any such files or software may be used only in ways that are consistent with their related licenses and/or copyrights

5. Creating and Capturing Records

Recordkeeping systems

In order to comply with statutory and regulatory requirements, it is important that records are captured into one of the official departmental recordkeeping systems so they can be located when required.

The purpose of creating and capturing records into a recordkeeping system is to:

- Capture information of evidential value;
- Facilitate effective searching and retrieval;
- Establish a relationship between that record, the creator and the business context that originated it; and
- Link them to other records, where required.

The official repository for departmental records is RecordsNI (HP Records Manager). Where RecordsNI is not suitable, i.e. linked spreadsheets, CAD drawings and maps etc, it is recommended that they are stored in a line of business application or in the DoF Data Centre.

*Records **cannot** be saved to C: drives as there is a greater risk of loss due to equipment failure.*

It is recommended that:

- records, irrespective of media or format, are captured into RecordsNI or other official recordkeeping system;
- rules should be applied to ensure an appropriate and consistent method of titling, indexing and other describing information (metadata) is devised and used for both paper and electronic records;
- the records are arranged according to functions rather than in a subject or organisational structure;
- procedures are put in place to ensure records are captured into recordkeeping systems by staff who work away from the office. All staff should comply with DoF's information security policies and be aware of the risks associated with the practice of using removable storage devices (such as IronKey) and downloading records on to DoF systems and equipment (e.g. laptop, BlackBerry). If staff use such devices, records must be captured into DoF's recordkeeping systems as soon as staff have access to the network;
- business areas should have procedures which clearly state what records may be taken off-site, under what circumstances this is permissible, how this information should be protected when off-site and how information created when away from the office should be captured into DoF systems; and
- recordkeeping systems are monitored to ensure staff are following proscribed procedures for capturing records.

Managing recordkeeping systems

Records should be arranged within a logical filing system, which should enable files and documents to be quickly located and retrieved and facilitate easy identification of records when they are due to be destroyed or permanently preserved.

The file plan is a mandatory corporate filing system throughout the Northern Ireland Civil Service. A file plan is a functional approach to file management. It reflects the functions, activities and transactions of the department rather than an organisational structure. Organisational structures are subject to change, whereas underlying business functions remain relatively constant, therefore providing greater business continuity.

In the DoF File Plan there are currently 7 corporate functions and 17 operational functions.

Corporate Functions

Corporate functions are those common to every NICS department and include all the general management activities and internal administration processes that keep departments running and support the business programmes and services.

The seven corporate functions which form the first level (or classification) of the file plan are:

- Accommodation & Services
- Audit & Accountability
- Financial Management
- Human Resource Management
- Information & Communication
- Strategic Management
- Technology & Telecommunications

Operational Functions

The first level of the file plan will also contain the department's main 'operational' functions. In this context 'operational' is used to describe those business functions that are not generally found in other departments but fall uniquely within a particular department's remit.

These areas of the file plan, as well as the corporate functions, will be developed as and when required and will be quality assured by PRONI.

File Plan Guidance
The file plan is a structured classification of records which provides full representation of the business of an organisation.

The top levels of the file plan, levels 1 – 3 are called ‘Classifications’, the levels below these classes are called ‘Book Levels’ and ‘Containers’.
The container is placed at the lowest level of the file plan and represents the file into which documents are placed.

When creating and filing information, staff will need to consider if the information is corporate or if it is directly related to their business function.

Some examples of corporate information and where it should be filed are as follows:

- *Stationery Orders*
  Accommodation and Services – Supplies and Services – Acquisition – Stationery
- *Parliamentary Questions*
  Information and Communication – Government Liaison – Parliamentary Questions
- *IT Work Request*
  Technology and Telecommunications – Application and System Support – Work Requests
- *Policy on Term Time Working*
  Human Resource Management – Policy Work life Balance – Flexible Working Arrangements – Term Time Working

Documents, or policy and procedures which are specific to a given area should be filed under the **operational function**. For example, while a policy on Term Time Working should be placed under Human Resource Management as it relates to all staff in the department, policy relating to Rating Reform should be placed under Rating and Valuation as it relates only to that operational area.

- *Rating Reform Implementation Policy*
  Rating and Valuation Services – Policy – Rating Reform – Rating Reform Implementation Policy.
- *Policy on EU Programmes relating to Finance*
  Government Finance Services – Policy – European Structural Funds – Building Sustainable Prosperity – EU Programmes Criteria.

Staff should ensure that guidance and direction is provided on the location that information should be filed in. For example, a project team working on a Remote Working project should advise staff that all relevant documentation should be filed under the classification of DF07/007/007/003 and its associated containers.

File Plan Administration
Responsibility for the administration of the departmental file plan will ultimately be assigned to DoF Information Management Unit.

Area of administration should include:

- Addition of containers
- Central monitoring on naming conventions for classifications, book levels and containers
- Central monitoring of categorisation of documents and naming conventions

Local administration will be carried out by Business Area Information Managers (BAIM's), Local Information Managers (LIM's) and Power Users who should monitor the use of the file plan within their business area and provide advice and guidance on naming conventions and requests for containers and book levels. On occasion, Business Areas may request containers to be created which are specific to their Line of Business. Should BAIM's identify documents which may have been inadvertently stored within such containers, they should liaise with individuals requesting them to be saved in a more appropriate location.

Requesting Containers

To submit a request for the addition of a container to the DoF File Plan:

- Staff must contact their Business Area Information Manager (BAIM) with a request for a container. The BAIM is responsible for approving the container. The BAIM should scrutinize the request to ensure that a similar container is not available; that the container is being requested in the correct area of the file plan and that suitable naming conventions are used for the creation of the container.
- If the BAIM is satisfied with the container request, they will pass it to Power Users for action.
- There is no requirement for Container Requests to be submitted to the Fileplan Mailbox for IMU approval. IMU will generate quarterly reports listing the Containers created for each Business Area and this will be forward to the BAIMs. In viewing these BAIMs should give attention to the titling and any restrictions on the Containers to ensure they comply with good records management practice

Requesting Book Levels

Fileplan Request procedures have been revised for Book Level requests to ensure any new Book Levels created in the Fileplan have the specified Retention periods added. IMU are required to retain a copy of new requests should there be occasion in the future if the retention/disposal of a book level is challenged.

The request template which has been revised and the following procedures will apply to all Book Level requests only.

- All Book level requests must be created using the Fileplan Request Template. (General email requests will not be accepted). A copy of this has been saved in Containers for each Business Area.

- Business Areas should ensure the completed request is captured in the relevant Business Area Container.
- The Retention/Disposal field must be completed and attention given as to whether access controls should be applied at Book Level or not. Requests will be returned if the field is not completed.
- The request form should be forward by the BAIM/PowerUser to the Fileplan Mailbox.
- IMU will assess the Book level request and if created confirmation will be forward to the BAIM.

IMU staff will monitor the mailbox regularly throughout the day to ensure that containers are added to RecordsNI as soon as possible. If a list of containers requests is received from a business area, IMU will approve the requests and return them to the Power User to be added to the file plan.

Deletion of classifications, book levels and containers

Deletions of categorisation within the file plan are carried out by Systems Administrators. If a deletion is required a work request should be submitted via the Touchpaper system. IMU must also be made aware of changes to file plan structure.

Monitoring File Plans

There will be a need to retain some central control over the file plan and the creation of containers within it, to ensure they are correctly named and positioned in the appropriate area of the file plan. Each business area should establish methods of monitoring the file plan on a regular basis and should provide guidance and training on the categorisation of documents as required.

Personal Containers

Personal Containers are an area is set up for each user (which is a Pink Folder). This is an area that should be used very selectively. The only documents that should be stored in this area are those that are of a truly personal nature. All DoF related documents should be stored into the File Plan, even if they are still being drafted. Note the following points:

- Personal container within RecordsNI is provided to all users.
- Personal container is a separate RecordsNI record type.
- The maximum number of documents a personal container can hold is 30.
- Personal containers are excluded from searches by anyone other than the owner, unless it is considered necessary for compliance or other reasons, such as the prevention or detection of illegal activities.

Metadata

This is information about documents or records. It is either automatically generated when a document is created or it may require the user to fill in

some fields. For example the metadata for a word document might include title, author, date created etc.

Metadata provides accurate and authentic contextual information about documents and must not be deleted from containers (even by system administrators) that have been identified for permanent preservation. Metadata for these containers will be managed (including retention or eventual destruction) as part of the agreed disposal scheduling process and by formal appraisal reports which will be completed with PRONI.

If containers have been identified for destruction after a set period of time in an agreed disposal schedule – documents (and associated metadata) can be sent to a 'temporary holding area' for final destruction (regular reports should be kept for possible review by PRONI). Any finalised records (and associated metadata) in these containers, must not be deleted (even by system administrators) for legal and auditing reasons and will be managed as part of the agreed disposal process.

Metadata can be captured in RecordsNI via record types – 2 standard record types will be established for all departments, ie. container and document. It is recommended that as many metadata elements as possible are captured automatically by RecordsNI to assist user acceptance of RecordsNI.

Although Departments will have the flexibility to capture specific metadata elements according to business needs (in different business related record types), they must also comply with any metadata standards set by Government requirements and PRONI. See Sections 3 and 21 for relevant web links.

Metadata also exists about the file plan, users, auditing and security permissions etc – this information requires careful management and documentation over time. Any Departmental restructuring or change in ownership that affects the 'class' levels of the file plan (ie. down to the 'book icon' in RecordsNI) will affect disposal arrangements and must be agreed in advance with PRONI (via reports, disposal schedules or appraisal reports).

Naming Conventions

Meaningful naming of documents and e-mails is essential, this will facilitate ease of reference as the name of the document will be the primary method used to search, locate and identify in the future. It is vital that when naming a document that it is:

- Descriptive and clearly identifiable – says what the document is about
- Specific – it distinguishes the document from others on the same topic.
- Consistent – it follows patterns and conventions which have been agreed by others for a particular topic.

Practices in Naming Documents

Do

- use sentence case for document titles.
- name your document so that the name is meaningful to others and can be easily located.
- provide keywords to the content of the document to facilitate searching.
- remove all instances of “FW”, “RE” and ‘HPRM’ from e-mail titles.
- if using a dash “ - “, include a space immediately before and immediately after the dash to enable proper searching within RecordsNI.

Don’t

- use capital letters.
- identify electronic file format information – for example e-mail, word document, Excel etc.
- include the date the document was created as this is automatically captured.
- use generic names like ‘Latest Version’; ‘Lecture’.
- base names on your ownership of the record, e.g. ‘Jenny’s documents’.
- use the words ‘Miscellaneous’ or ‘General’, as these encourage poor filing practice.
- compress two or more words into one word, e.g. ‘CorpSer’ or ‘RecordMan’. Always separate words with spaces and type out in full.
- avoid using special characters such as semi-colons, slashes or underscores as this can affect the quality of the search.
- automatically accept the e-mail subject as a name – it is likely that you will have to rename emails with an appropriate title.
- best practice would suggest that users should refrain from using the following characters in a name: \ / > < * ? “ ; : _ these symbols can affect the quality of the search. However there may be occasions where it is necessary to use such characters in the titling of documents i.e. to separate parts of a name for clarity. In such cases space-dash-space (-) should be used.

Acronyms

As much as possible avoid the use of acronyms. This will improve your search for a document and will assist users who are not familiar with the topic to understand what it refers to. Sometimes there are acronyms which are indispensable and which are more recognisable than the full title, e.g. MLA, DoF, DAERA, NISRA. Where possible use the full title and err on the side of caution.

Version Control

When saving a document, the use of consistent numbering of versions will enable staff to differentiate between drafts and approved versions and enable easy identification of the most recent copy. The same approach to numbering

documents/records should be applied across the whole department. A new version is created when a change occurs that alters the document in a material way. Changes to correct spelling mistakes and such like aren't sufficient to warrant a new version.

DoF documents should include a 'v' followed by a number. For drafts the number should increase after the point and for reissues of approved versions it should be shown by an increase before the point, e.g.

- v0.01 first draft
- v0.02 second draft
- v0.03 third draft
- v1.0 first approved and published version
- v1.01 update to approved version but not published so again in draft form
- v1.02 second draft of update to approved version but still not published
- v1.1 published version of updates
- v2.0 second reviewed, approved and published version

The draft document becomes a formal record at the point of when it is approved and/or released. It is advisable at this point to make the record "read-only" by finalising it and thereby ensuring accidental alterations do not happen.

Email management
Users should refer to, and ensure they are familiar with, existing departmental guidance in the Records Management Policy Statement.

A 3 month rule will be imposed on all email accounts. All emails should be saved into RecordsNI as soon as possible after being received or deleted if not relevant for business purposes. An email is important if it:

- Has long term administrative or historical value.
- Includes evidence of business activities or transactions.
- Contains information, advice or explanation not duplicated elsewhere.
- Relates to decisions taken and has evidential value.
- Was drafted as a result of policy or legislation.

Emails that have not been saved into RecordsNI and remaining within the native email application will be automatically deleted from inboxes and associated folders, sent items and deleted items after 3 months.

Staff should ensure that e-mail delegation is given to additional, appropriate members of staff to ensure that e-mail accounts are addressed and managed in accordance with three month rule.

For those emails that are evidence of a decision or a business transaction and therefore need to be retained as a corporate record, the following general guidelines apply:

- For sent emails, whether internal or external, the sender should save the email in the appropriate part of the file plan;
- For external emails received by one person, the recipient should save the email;
- For external messages received by more than one person, the individual with responsibility for the area of work relating to the message should save the email (assuming they are one of the recipients). Where this is not clear it may be necessary to liaise with other recipients.
- If an external message has multiple recipients and relates to more than one area of work then the first recipient should save it and others should create links to the saved RecordsNI document.
- For conversation strings (where an email 'conversation' is ongoing between a number of individuals), wait until the dialogue has finished or has settled at a reasonable point before saving into RecordsNI and name appropriately.
- Where attachments are received with an e-mail, the email message and attachment should be saved together. The name of the attachment should be left unchanged (regardless of naming conventions) as it will be referenced in the main body of the e-mail message. It may however be necessary to re-name the e-mail to ensure that it can be readily identified.
- Where the e-mail message does not contain relevant information (i.e. there is no information contained in the e-mail message other than the attachment) it should be noted that the main body of the e-mail may be evidence of when and to whom a document was sent and so, for completeness, may need to be retained.

Saved emails will often need to be renamed to something meaningful. You do not have to accept the name in the subject field, however it is good practice to copy the original email name or subject line into the document notes field. This will aid retrieval via searching at a later date.

Titling of Emails should also be considered in conjunction with the guidance on naming conventions. The name does not need to duplicate information already identified with the email (such as sender, date sent, recipient, date received etc) as these will be automatically generated by RecordsNI. The title should not include the automatically generated 'FW', 'RE' or 'HPRM Ref'.

Where attachments are received with an email, the email message and attachment should be saved together. The name of the attachment should be left unchanged (regardless of naming conventions) as it will be referenced in the main body of the email message.

Sending Attachments
There should, in most instances, be no need to send electronic document attachments internally to staff. Only a link to the document within RecordsNI needs to be sent. This will cut down on the size of emails being sent throughout DoF and will therefore reduce the volume of network traffic.

Where emails are being sent to recipients outside the NICS, electronic document attachments will always need to be used.

Where an attachment is being sent to both internal (using RecordsNI) and external users then both the RecordsNI link and electronic document options must be selected.

Ensuring Completeness

The Department needs to be able to provide a complete and verifiable record of its business activities and therefore needs to be able to demonstrate a complete event or transaction from start to finish and all important stages in between. All staff should be aware of their responsibilities in ensuring accurate and complete records. If a record is incomplete it has no legal standing in a court of law. The following are some examples of complete records:

- Complete records of a meeting might include:
    - the agenda, minutes, any papers tabled at the meeting and circulation lists.
- Complete records of project work might include:
    - Authorisation for events or transactions, including emails, minutes and documents requiring signature;
    - Records that demonstrate how decisions were arrived at, including reports, minutes and advice;
    - Business cases, progress reports, risk analysis, plans and specifications.
- Complete records of a report would include:
    - The final report, important stages in its drafting, working papers relating to it, sent in support of, or as evidence that targets have been met.

Department of
Finance
An Roinn
Airgeadais
www.finance-ni.gov.uk

Department of Finance
Records Management Policy

Implementation Date: 1 September 2016

Next Review Date: 1 September 2019

Introduction

1. The Department of Finance (DoF) is an information-based organisation. The service that it delivers to its customers, whether internal or external, depends on its efficiency in creating, using and storing information. Records must meet legislative, operational and archival requirements and support accountability in decisions taken by the organisation. It is therefore vital that management of this information is prioritised as an administrative discipline, which controls all aspects of the record from creation through to disposal in an appropriate manner.

Overall Commitment

2. The Department is committed to providing and complying with effective records management procedures which are integrated as key activities within the organisation by ensuring that:

    - the creation, management, review and disposal of records is carried out in a manner which accurately documents the functions of the organisation and is compliant with associated policy;

    - the records management function supports the regulatory environment within which it operates;

    - procedures, guidance and training are available to assist staff in producing records which reliably represent accurate information that was used in, or created by, the business process and which will enable integrity and authenticity to be demonstrated;

    - activities relating to records management from creation to disposal are adequately resourced, managed and monitored;

    - appropriate security measures are in place for storage, management and transportation of sensitive departmental information;

    - the departmental file plan is managed and maintained to retain records in a structured manner;

    - Information Asset Owners are appointed to each business area to ensure that departmental information assets are accessed, controlled and managed accordingly; and

- appropriate and secure procedures and processes are in place for sharing of information.

Role of Records Management

3. Records management is the term used to describe an administrative system by which the organisation seeks to control the creation, retrieval, storage, preservation or disposal of its records.

4. A record can be described as recorded information, in any format or media, created or received and maintained as evidence by the Department in the transaction or pursuance of business.

5. Effective records management will enable the Department to:

    - access records when required, providing timely information for operational need;
    - provide secure and legally admissible records demonstrating accountability;
    - ensure records, particularly those containing personal or sensitive information, are not retained for longer than is legislatively, legally or administratively necessary;
    - store historical records of past activity to provide a corporate memory;
    - make better use of space and storage facilities both physically and electronically;
    - optimise use of staff time;
    - improve control over records;
    - comply with legislation and departmental policy; and
    - reduce costs.

Responsibilities

6. *All staff*
   All staff in the department are responsible for:

    - ensuring they have a clear understanding of records management and demonstrate commitment to duties relating to record keeping;
    - creating records which are consistent, reliable, accurate and complete;
    - identifying records which should be captured because of their business function or content;

- recognising e-mails which are records and filing accordingly;
- capturing records which authentically document activities in the course of which they were produced;
- storing records in the appropriate area of the file plan within the Records NI system and in physical storage;
- applying security and access controls to records, where appropriate;
- ensuring that searching, viewing and browsing records is done only for departmental business purposes;
- finalising documents when appropriate to ensure they become departmental records; and
- applying appropriate disposal and retention actions to records based on the departmental Retention and Disposal Schedule.

Recordkeeping responsibilities should be defined, agreed and documented in Personal Performance Agreements as well as contracts relating to service provision on behalf of DoF, when working in partnership with both internal services and external bodies.

Records management training needs should be analysed by line managers, particularly if staff are finding it difficult to fulfil their records management responsibilities because they do not have the necessary records management skills or guidance.

7. *Business Area Information Managers*
Business Area Information Managers (BAIMs) co-ordinate the compliance and monitoring of the records management policies and procedures throughout the Department. BAIMs may transfer or delegate some responsibility to appropriate members of staff within their business area.

8. *Departmental Information Manager/Records Manager*
The Departmental Information Manager (DIM) and the Records Manager produce records management policies and procedures. They also co-ordinate the compliance and monitoring of those policies and procedures throughout the Department through the BAIMs.

9. *Information Asset Owners*
Information Asset Owners (IAOs) are senior members of staff involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result, they are able to understand and address risks to the information, ensure

that information is fully used within the law for the public good and provide written input to the SIRO on the security and use of their asset. Business areas need to be able to demonstrate progress in:

- enabling staff to conform to the records management standards;
- identifying resource requirements; and
- areas where organisational or systems changes are required.

10. *Senior Information Risk Officer*
The Senior Information Risk Officer (SIRO) has overall responsibility for the organisational function of records management.

Statutory and Regulatory Environment

11. There are a number of pieces of legislation which impose the need for effective management of all Departmental records, both paper and electronic

12. The records of DoF, like those of other Departments, are public records under the terms of the Public Records Act (NI) 1923. It is therefore a legislative requirement for the Department to implement records management as set out in this Act and in the Disposal of Records Order (S.R. & O. 1925 No.167). The legislation lays down the procedures both for the destruction of records deemed to have no long-term value and for the preservation and transfer to PRONI of records selected for permanent preservation.

13. The Freedom of Information Act 2000 (FOIA) provides a statutory right of access to information held by public authorities (subject to exemptions). Public authorities are obliged to comply with the Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000, which is intended to support the objectives of FOI legislation by outlining the management practices that should be followed by public authorities in relation to the creating, keeping, managing and disposal of their records. All information held by the Department is subject to the FOIA. No distinction is made regarding information held in remote locations or offsite storage. Staff should ensure that they are familiar with the content and requirements of the DoF Freedom of Information Policy Statement.

14. The Data Protection Act 1998 (the DPA) entitles individuals to access their personal information, which is being processed by another, on request. The Department is committed to managing records and applying appropriate security measures in compliance with the principles of data protection and in line with DoF Data Protection Policy Statement.

15. Environmental Information Regulations 2004 (EIR) stem from European rather than national legislation. EIRs provide the public with

a statutory right of access to environmental information held by public authorities.

16. Each business area should also consider and take into account any legal or regulatory obligations specific to their function.

Access and security

17. Whilst departmental policy places emphasis on open and transparent information, there are occasions when staff should consider if any of the information held within a document or file/container needs to be limited to a specific group of staff or, exceptionally, to only one or two individuals.

18. The Department remains committed in delivering openness and transparency of information, but is equally protective in ensuring sensitive information is appropriately restricted and only accessible to the relevant groups or business area.

19. Compliance checks will be carried out to ensure sensitive/personal information is appropriately restricted. Where access controls have not been appropriately applied to sensitive/personal Information, staff may be challenged.

20. Audit logs will also identify inappropriate viewing, previewing and/or editing of such information. The titling of some documents can clearly distinguish them to be personal or sensitive however, on occasion, these documents may have inadvertently not had the appropriate access controls applied. Staff must not view, preview or and/or edit such documents, but should inform their line manager or BAIM who will liaise with DoF Information Management Unit.

21. Staff are personally responsible for the safe-keeping of personal data in their possession and should ensure this is only accessed and processed in line with business need. Staff should also be aware that they must not search for or view information which is not appropriate to them or their business area. Any staff viewing or carrying out excessive searches for information (personal or otherwise) will be challenged and may face disciplinary action.

Responsibility for Historical Records

22. A record becomes historical when it reaches 20 years old and has been deemed to have permanent value for legal, administrative or research purposes. These records will be protected by the Department in consultation with the Public Record Office of Northern Ireland (PRONI).

23. The records selected for permanent preservation are outlined in the DOF Disposal Schedule and transferred to PRONI. Before transfer

can take place, the records must be reviewed under Part VI of the Freedom of Information Act 2000 (FOIA). Once transferred, these records become the responsibility of PRONI.

E-mail

24. The principles of this policy apply equally to e-mail and it is necessary to transfer e-mails relating to business activity and transactions to the appropriate area of the file plan within the Records NI system to ensure a complete and accurate representation of the record.

25. A 3-month rule has been imposed on all e-mail accounts. E-mails that have not been saved into Records NI system and remain within Outlook will be automatically deleted from mailboxes and all associated folders after 3 months.

Policy Awareness

26. A copy of this policy statement must be provided to all new members of staff and interested third parties. Existing staff and relevant third parties will be advised of the policy which will be posted on the Departmental intranet site and will be available through the publication scheme, as will any subsequent revisions. All staff and relevant third parties must be familiar with and comply with the policy at all times. This policy will be reviewed every three years, at a maximum.

Further Information

27. Any queries about information access legislation in the Department should be addressed to the relevant Business Area Information Manager or the Information Management Unit. Further information can also be provided by the Information Commissioner's Office.

Associated Documentation

28. This policy should be read in conjunction with:

- DoF Data Protection Policy
- DoF Access to Information Policy
- DoF Information Security Policy
- Departmental Guidance on Data Sharing

29. Copies of all these policies are available on DoF's internet and intranet sites.