POLICY ON SENDING INFORMATION OUTSIDE INVEST NI

1. INTRODUCTION

1.1 This policy must be followed when sending any **personal or business sensitive** information to a party outside Invest NI. This includes External Delivery Organisations, Contractors, Stakeholders, Customers etc.

1.2 Personal or business sensitive information must never be sent externally via standard email, except as permitted in 1.3 below.

1.3 Any information being sent to a NICS Department can be sent securely from your Invest NI email account. This includes all emails sent to DfE. If the information you are planning to send to a NICS Department cannot be sent via email then the procedure in this policy must be followed.

1.4 Any party not contracted through Central Procurement Directorate (CPD) who is being given access to personal or business sensitive information held by Invest NI that does not relate to them must sign the Invest NI Third Party Data Processing Agreement (See Intranet).

2. PURPOSE

2.1 The purpose of this policy is to ensure the security and confidentiality of information whilst it is being sent to appropriate parties outside Invest NI.

3. CONFIDENTIALITY OF INVEST NI PERSONAL AND BUSINESS SENSITIVE INFORMATION

3.1 Invest NI's processing of personal information must comply with Data Protection laws. Please see Invest NI **Data Protection Policy** for further details.

3.2 Prior to making arrangements to provide a third party with personal or business sensitive information held by Invest NI that does not relate to them, a contract must exist to state the purpose for which access to this information is being granted. For most Contractors this will be the Contract made through CPD or the internal Procurement process. For all other third parties a 'Data Sharing Agreement' must be signed.

3.3 Such agreements must be signed on behalf of Invest NI at Director level in line with all other legal agreements and they must state a 'permitted purpose' for which Invest NI is providing the information to

the third party. The purpose must be in line with the purpose for which Invest NI collected this information from the Data Subject. If the purpose does not correspond to the reason Invest NI collected the information then Invest NI must seek consent from the relevant Data Subject(s) affected prior to release of their information.

3.4 Consideration must be given to the geographical destination in each case of information transfer because personal data may not be transferred to people or organisations situated in countries outside the EEA without adequate protection. Refer to the **Procedure for International Transfers** for further information.

4. SECURITY AND CONTROL

4.1 As Data Controller Invest NI must ensure the security of information being provided to other parties. This includes ensuring the secure sending (transfer) of the information.

4.2 Although there are other ways to *receive* information there are five methods of *sending* personal and business sensitive data approved by Invest NI:

(i) Invest NI **Office 365** account
(ii) Secure email service '**mimecast**'
(iii) Secure **USB DataLocker** device
(iv) Invest NI issued **Encrypted Mobile Phone**
(v) "Signed For" **Recorded or Special delivery** post

4.3 Staff should decide on the most appropriate method of transfer to suit their business need from the above options e.g. the DataLocker USB stick or an Invest NI encrypted phone may be most appropriate for delivering presentations that contain business sensitive information, whereas 'mimecast' may be most efficient for the transfer of large files within a tight timescale.

4.4 Whereas cloud based services not noted above may be used to **download** information from external parties this can only be accommodated on a case by case basis after obtaining approval from the Information Governance Team (via privacy.officer@investni.com) and completing the website access request form (if prompted by the Web Filter). **Non approved applications or accounts must not be used to upload or send information**.

4.5 Records of all information uploaded must also be saved in appropriate Meridio file plan folders in line with the Invest NI **Records Management Policy**.

5. APPROVED ELECTRONIC SOLUTIONS

5.1 Office 365 solution

5.1.1 An Office 365 portal is a secure method for Invest NI led groups to share information. Information is uploaded to a secure portal and members of the group can access and download securely.

5.1.2 Access to an Office 365 account can only be granted following approval from ICT. Please contact the ICT service desk for further information and suitability.

5.1.3 Other cloud based services may be used to **download** information from external parties only. They must **not** be used to upload or send information – see paragraph 4.4.

5.2 Use of 'mimecast' secure email service

Technical guidance on how to use the service will be provided directly by ICT.

5.2.1 Mimecast is a secure method of sending emails and large file attachments.

5.2.2 Please see the dedicated intranet page with detailed instructions on how to use this secure email service.

5.3 Use of secure USB DataLocker device

Requests for a secure USB DataLocker device should be made by logging an ICT Service Desk call (ext 140 or ICTservicedesk@investni.com). The steps that must be taken to ensure the safe transfer of electronic personal and business sensitive information are as follows:

5.3.1 Data is transferred from Invest NI's system onto a secure DataLocker USB device;

5.3.2 An arrangement is made with the recipient for collection of the DataLocker device;

5.3.3 Password for access to the DataLocker device's contents is given to recipient over the telephone when they are ready to transfer information onto their systems;

5.3.4 The recipient confirms transfer of data onto their systems;

5.3.5 Arrangements are made for return of the DataLocker device to Invest NI;

5.4 **Use of Invest NI issued encrypted mobile phone**

5.4.1 Technical guidance on how to use an Invest NI encrypted mobile phone to securely transfer information is available on the intranet.

5.4.2 Unless officially issued by the ICT team other mobile devices should **NOT** be used to transfer information.

6. POST

6.1 Staff should give due consideration to any information that they intend to send by traditional post. Sensitive personal and business information should only be sent via post in exceptional circumstances and by the following methods:

6.1.1 Sensitive personal and business information should be sent via “Signed for” recorded or special delivery to enable its progress to be tracked and receipt to be confirmed.

6.1.2 For heavy/bulk postal items, where prudent, a courier who can confirm secure delivery [in writing] may be used.

6.2 For the purposes of this policy, exceptional circumstances are deemed to be those where the information cannot be scanned and sent in a secure electronic manner as per the processes above.

6.3 Staff are reminded to ensure that the postal address of the intended recipient is correct before items of post are dispatched via the FM Contractor.

7. Transfer of Physical (paper-based) Files

7.1 Whenever possible physical information should be converted to electronic information (by scanning) to share with recipients per the procedure above. When this is not practical (e.g. the Northern Ireland Audit Office or other contracted auditor may require access to numerous historic files), the process set out in paragraph 7.3 below should be followed. Please refer to the **Records Management Policy** regarding the lifecycle of records to ensure that files are not kept for longer than is necessary.

7.2 When arranging collection and return of physical (paper-based) files it is the responsibility of the staff member co-ordinating the transfer, to

liaise directly with the recipient, and to be present during the collection and return of files.

7.3 The steps that must be taken to ensure the secure transfer of physical personal and business sensitive information are as follows:

7.3.1 Information (files) is listed to ensure that Invest NI has a full record of files being provided to the recipient;

7.3.2 Either (i) the recipient comes to Invest NI to collect files or (ii) Invest NI delivers files to the third party. Use of a courier is not recommended unless they can confirm secure delivery;

7.3.3 The recipient signs for the files listed, acknowledging the receipt of information as listed in paragraph 7.3.1 above;

7.3.4 The recipient returns files. Invest NI checks the returned files against the list of files provided to the recipient. If all files are present, confirmation of receipt of files is provided to the recipient (if requested) and a copy is kept for Invest NI records;

7.3.5 If all files are not present Invest NI should only acknowledge receipt of files that are returned. The recipient should be notified of the missing file(s) in writing as soon as possible and a search for any missing file(s) should be instigated. If files are not found then an incident should be reported as per the **Data Breach Management Policy**.

8. OWNERSHIP

8.1 It is the responsibility of each member of staff to ensure that any information they wish to share with an outside party is shared in line with the **Data Protection Policy** and that the transfer itself is in line with this policy.

8.2 This policy forms part of the Information Security Handbook and should be read in conjunction with the relevant policies contained therein. Any further clarification required concerning this policy can be sought from the Information Governance Team at privacy.officer@investni.com.

Version Control

Version	Author / Reviewer	Review Date	Approved by
1.0	Danny Smyth	4 September 2009	Information Security Forum
2.0	Danny Smyth	2 February 2010	Charles Hamilton
3.0	Danny Smyth	10 October 2011	Charles Hamilton
4.0	Danny Smyth	21 January 2013	Steve Chambers
5.0	Danny Smyth	01 December 2014	Nigel McClelland
6.0	Danny Smyth	10 November 2016	Nigel McClelland
7.0	Mark Hutchinson	26 February 2019	Danny Smyth