Bring Your Own Device Policy

Issued by: Information Standards, Governance Services

Approved Policy

Table of Contents

1. *Introduction*

The Northern Ireland (NI) Assembly Commission (the Commission) recognises that Secretariat staff have personal mobile devices such as smartphones and tablet devices that they may wish to use for business purposes. In permitting such use, the Commission recognises the need for a framework within which the use of mobile devices will be managed.

2. Policy Statement

2.1 The Commission's 'Bring Your Own Device' Policy sets out a framework within which the Commission will manage the use of personal mobile devices by secretariat staff for work purposes. The policy describes the security procedures and controls required for the use of personal mobile devices within the Secretariat.

2.2 The use of personal mobile devices for business purposes gives rise to increased risk in terms of security of our IT resources and communications systems, the protection of confidential and proprietary information and reputation, and compliance with legal obligations.

2.3 **No one is required to use their personal mobile device for business purposes.** It is a matter entirely for each person's discretion and must be authorised by Director / Head of Business.

2.4 Where a Head of Business deems it necessary for a member of staff to have remote access to Assembly email, they should in the first instance consider applying to the Director of Facilities for the use of an Assembly smart phone for business use. Staff already in receipt of an Assembly smart phone should not normally require access to Assembly email from a personal device.

2.5 If you wish to apply to use a privately owned device you will need approval before submitting your request to the IS Office. Both you and your Head of Business/Director must sign the agreement form in this policy. Where a Director / Head of Business deems it necessary and has provided their written approval, staff may use a personal mobile device for business purposes, provided they sign the declaration attached at the end of this policy. There is a limit of one personal device per person. Only in exceptional circumstances will access to more than one personal mobile device be facilitated.

2.6 This policy should be read in conjunction with the following Commission policies:

Commission IS Security Policy;
NI Assembly Security Policy,
Policy for the use of IT Resources;

Assembly Mobile Phone Policy;
Password Policy;
How to change Mobile Phone Email Synchronisation Password;
Information Assurance Policy;
Email Management Policy;
Retention and Disposal Policy; and
Assembly's Data Breach Management plan.

2.7 This policy covers all Assembly Secretariat staff, inward secondees and agency workers. The policy refers to access to the NIAC mailbox and internet using a personal mobile device. Access to other network information systems will not be provided through personal devices.

2.8 The NIAC accepts no responsibility for privately owned mobile devices. Although every effort will be made to ensure that connection via the Activesync functionality will not cause harm, the NIAC accept no liability for any loss of privately owned data as a result of connection, or other associated functionality, including any consequences of viruses or malware.

3. Purpose of the Policy

3.1 The purpose of this policy is to protect the Commission systems and data and to prevent data from being deliberately or inadvertently lost, disclosed or altered, while enabling Secretariat staff to access Commission systems using a device. This policy sets out the circumstances in which we may monitor access in order to protect the Assembly's IT resources from misuse and ensure the availability and integrity of Assembly information held electronically. It will also protect authorised users from misguided or ill-informed access to, or processing or storage of, information that may be inappropriate or illegal. This policy sets out the action which we will take in respect of breaches of this policy.

3.2 The main objectives of the Bring Your Own Device Policy are:

- To provide access to the Commission email system in a way that facilitates Commission business;
- To ensure that appropriate levels of security are in place to maintain the confidentiality, integrity and availability of information;
- To preserve the confidentiality and integrity of information;
- To protect against unauthorized access to information;
- To establish procedures in the event of loss / theft of personal devices covered under this policy;
- To define individual responsibility and accountability, in order to maintain the protection of information.

4. Policy Scope

4.1 The policy applies to use of personal devices for business purposes both during and outside office hours and whether or not use of the device takes place at your normal place of work or elsewhere.

4.2 The policy applies to all personal mobile devices used to access the Commission resources and communications systems which may include smartphones, mobile, tablets and laptop or notebook computers.

4.3 This policy covers all Assembly Secretariat staff, inward secondees and agency workers. The policy refers to access to email using a personal mobile device. Access to other network information systems will not be provided through personal devices.

4.4 When Secretariat staff access the Commission system they may have access to email containing confidential or personal data. Such data may include for example - HR or staff issues; commercially sensitive information relating to Assembly procurements or other potentially sensitive or embargoed/classified information. It is therefore important for staff to refer to Point 5 of the Record and Email Management Policy as follows:

> "It is therefore important that Email containing personal, sensitive or classified information (in accordance with the Information Assurance Policy) must not be retained in the mailbox. Email containing personal data should be dealt with immediately. If the email is required as a record it should be filed appropriately. If the email is not relevant for business purposes it should be deleted."

4.5 The use of personal devices providing access to such data exposes the Commission to a number of risks, including those arising from the loss or theft of the personal device. This could result in unauthorised access to Commission systems or data, the threat of malware (such as viruses or other threats that could be introduced into our systems via a personal device) and the loss or unauthorised alteration of Commission data (including personal and confidential information which could expose us to the risk of non-compliance with legal obligations of confidentiality, data protection and privacy). Such risks could result in damage to the Commission systems and reputation.

4.6 Breach of the policy may lead to the Commission revoking staff access to our systems from personal devices. It may also lead to action under the Commission's Disciplinary Policy, irrespective of whether the breach occurs during or outside office hours or where the breach takes place. Staff are required to co-operate with any investigation into a suspected breach, which may involve providing the Investigating Officer with access to the personal device and any relevant passwords and login details.

4.7 Through monitoring of centralised Commission systems and services such as internet and email, the Commission reserves the right to monitor such activity. In consultation with the device owner, this may involve the identification, review or erasing of content on the personal device **that is intended for Assembly use** or for use on its behalf.

5. Connecting devices to our systems

5.1 Connectivity of all personal devices is centrally managed by the IS Office, who must receive the necessary approval to use a personal device before it can be

connected to the Commission system. Personal devices must therefore comply with the Commission's Bring Your Own Device Policy. Secretariat staff must seek authorisation from AG4 or above and submit their request to the IS Office for consideration.

5.2 Some personal devices may not have the capability to connect to Commission systems therefore IS Office is not under any obligation to modify systems or otherwise assist staff in connecting to Commission systems.

5.3 The IS Office reserves the right to refuse or remove permission for your personal device to connect to Commission systems. The IS Office will refuse or revoke such permission where in our reasonable opinion a personal device is being or could be used in a way that puts, or could put, the Commission systems or staff at risk or that may otherwise breach this policy.

5.4 In order to access Commission systems, it may be necessary for the IS Office to install software applications on your personal device such as Activesync. If users disable or remove any such software, access to Commission systems may also be disabled.

5.5 In permitting staff to use personal devices for work purposes, personal devices must not be used in contravention of related IT policies - (see Section 2.6).

5.6 Once personal devices have been configured, information regarding access configuration settings must not be shared with anyone.

5.7 Staff must ensure that Activesync is disabled before work is carried out on a personal mobile device. Staff must also ensure that no transfer of Assembly information is made to "local" directories or other removable storage such as SD cards etc. where it may potentially allow unauthorised access if the personal device is lost or stolen.

5.8 Clear distinction must be made when using personal devices and Secretariat staff should not use personal email accounts for any transfer of Assembly information. Further information can be obtained in the Assembly Information Assurance Policy.

6. Monitoring

6.1 The contents of the Commission systems and data are property of the Commission. All materials, data, communications and information, including but not limited to email (both outgoing and incoming), during the course of business or on behalf of the NIAC is property of the NIAC, regardless of who owns the device.

6.2 In consultation with the device owner, and in order to protect NIAC systems, it may be necessary to monitor, identify, review or erase content. Staff are

advised not to use the Commission systems for any personal matter intended to be kept private or confidential as staff should have no expectation of privacy when using the Commission systems for any personal matter.

6.3 Monitoring, identifying, reviewing or erasing of content will only be carried out for legitimate business purposes, in order to:

- Prevent misuse of the personal device and protect Commission data;
- Ensure compliance with Commission standards of conduct and policies in force (including this policy); and
- Ensure that staff do not use Commission facilities or systems for any unlawful purposes or activities that may damage our business or reputation.
-

7. Security Requirements and Procedures

7.1 Minimum security measures - When using personal mobile devices to access Assembly email accounts, staff must apply appropriate security measures to prevent unauthorised access to the device. This should include as a minimum,

- Setting a password or PIN to unlock the device when not in use.
- Setting a timeout to lock the device after a period of inactivity. Recommended 5 minutes maximum.

7.2 Additional security measures such as Mobile Device Management (MDM) software should also be considered. These systems allow users to remotely trace the location of the device and disable / wipe content in the event of the theft or loss of the device. Given the wide range of devices and operating systems available for personal mobile devices, IS Office cannot provide a definitive list of recommended security measures, however staff in the IS Office will provide general advice on personal mobile device security on request. (Please note: some MDM products may incur costs to download and install. The Assembly will not fund or reimburse any costs associated with the installation of MDM software however depending on operating system, IS Office can provide advice on the availability of free MDM products.) Some devices, particularly older models, may not be technically compatible. If you need further information regarding technical requirements, please contact the IS Office.

7.3 In the event of the loss or theft of a personal device, or where a staff member believes that a personal device may have been accessed by an unauthorised person or otherwise compromised, the staff member must report the incident to the IS Office immediately. (Tel: IS Office Service Desk -028 905 21000 or email ITHelpDeskEmail@niassembly.gov.uk). IS Office can disable the Activesync software which will prevent the device being used to send or receive further email. Staff are also advised to refer to the Data Breach Management Plan for the loss reporting process. Staff are also advised to immediately change their network password to prevent further unauthorised access to the mailbox. Once Activesync is disabled only mailbox content

(emails, contacts and calendar entries etc.) which are already received on the device can be accessed. Depending on the mobile device, MDM software may allow for remaining Assembly data to be deleted remotely. IS Office can provide advice in such circumstances. Please note: When using MDM remote-wipe facilities, all phone data (including personal photos, videos etc.) may be permanently deleted. It is your responsibility to ensure that you regularly back up your private data.

7.4 Before passing or selling your personal device on to any third party you are required to inform the IS Office who will disable the connectivity to ActiveSync. Staff must ensure that Assembly mailbox data is completely erased before they donate, resell or recycle an old device, as these may retain access to Assembly information. Staff should familiarise themselves with the 'factory reset' option in the device settings. If in doubt, staff should consult IS Office for advice on erasing Assembly data.

7.5 Similarly, damage or faults requiring repair to personal devices should be brought to the attention of the IS Office in the first instance. The personal device must not be accessed or examined by any third party before seeking advice from the IS Office. **Should the device require repair, if possible, please consult the IS Office for advice on removing Assembly data prior to providing to any third party for repair or examination.**

7.6 Procedure on termination of Employment - In the event of staff leaving Assembly employment, on the last day of work all Commission data and any software applications provided by the NIA for business purposes must be removed from the personal device and access to Commission systems withdrawn. Staff should contact IS Office (Tel: IS Office Service Desk -028 905 21000 or email ITHelpDeskEmail@niassembly.gov.uk) to ensure that this process is completed before leaving Assembly employment.

7.7 Appropriate Use - Secretariat staff should not access or use Commission systems or data through a personal device that breaches any other relevant Assembly policies including those noted in Section 2.6.

8. Smartphone Security

Please see a link to the Information Commissioner's Guidance regarding Smartphone Security. This guide provides advice on the following:

1. Guarding your phone and setting PINs and passwords

2. Taking precautions in case your phone is lost or stolen

3. Smartphone's security settings

4. Back up and securing data

5. Installing Apps

6. Using antivirus software

7. Using software to find or erase your phone if it goes missing

8. Clearing your phone before you dispense with it

9. Accepting updates and patches

9. Accountability of behaviour - Declaration and agreement

I [name] request to use my personal mobile device for business purposes and explicitly confirm my understanding and agreement to the following:

- I have read, understood and agree to all of the terms contained in the Bring Your Own Device Policy.
- I have read and understood the Email Management Policy and agree to all the terms of the policy including ensuring all personal, classified and sensitive information is not retained in the mailbox but is stored securely and appropriately, in line with NIA policy.
- I understand that the terms of this policy will apply to me at all times, during or outside office hours and whether or not I am at my normal place of work.
- I acknowledge and agree that authorised personnel of the Commission shall have the rights set out in this policy, including but not limited to the right to access, monitor, review, record and erase data contained on my personal device (which I acknowledge may result in inadvertent access to or destruction of my personal data).
- I understand and agree that the Commission in its discretion may amend, or remove this policy at any time and that I will be bound by the terms of the policy as amended.
- I understand and agree not to share or communicate the NI Assembly remote access configuration information.
    - I understand and agree to ensure to apply appropriate security measures to prevent unauthorised access to my personal device

approved for work purposes. As a minimum this will include: Setting a password or PIN to unlock the device when not in use

    - Setting a timeout to lock the device after a period of inactivity (recommended 5 minutes maximium)

- I agree to immediately report to the IS office the loss or theft of a personal device, or where a personal device may have been accessed by an unauthorised person or otherwise compromised.

- I agree to immediately change my network password if advised, to prevent further unauthorised access to the mailbox.

- I agree to inform the IS Office before passing or selling my personal device on to any third party in order to disable the connectivity to ActiveSync. I will ensure that Assembly mailbox data is completely erased before I donate, resell or recycle an old device, as these may retain access to Assembly information. I agree to familiarise myself with the 'factory reset' option in the device settings and if necessary, I will consult the IS Office for advice on erasing Assembly data.

- I agree that any damage or faults to my personal device which require repair must be brought to the attention of the IS Office in the first instance. I understand that the personal device must not be accessed or examined by any third party before seeking advice from the IS Office to ensure Assembly data is removed prior to providing to any third party for repair or examination.

- I understand and agree that in the event of termination of employment, I will contact the IS Office on the last day of work to ensure all Commission data and any software applications provided by the NIA for business purposes are removed from the personal device and access to Commission systems withdrawn.

- I have read and agree to comply with the smart phone security guidance at paragraph 8 of the policy
- Please confirm if MDM software has been installed YES/NO
  (see paragraph 7.2)

USER DETAILS:

SIGNED

PRINTED NAME

_____

DATE

_____

HEAD OF BUSINESS / DIRECTOR PROVIDING AUTHORISATION:

SIGNED

PRINTED NAME

_____

DATE
