Acceptable Use Policy (AUP) for receiving emails on mobile devices

Employee: Please read this Acceptable Use Policy (AUP) thoroughly and forward the document in an email with a note agreeing to the terms to your manager for approval.

Manager : Please forward the email from your employee to the helpdesk confirming that you approve of access to the email system from a mobile device for your employee. In doing so you agree to the potential additional cost that may be incurred. If you are not familiar with the content please also read the document in full.

In order to increase choice, deliver a more satisfying user experience of IT services and as part of the wider move towards offering different modes of working, Global Information Services (IS) makes e-mail directly available across corporate and personal devices via the Exchange ActiveSync (EAS) service. In providing this facility, National Grid data will reside on the device and it is therefore necessary to put in place security controls to protect NG data.

This agreement provides the terms and conditions that govern access, management and support of the device and National Grid data stored on the device. The use of this service will be taken as you have read and you agree to adhere to the policies, terms, and conditions referred to in this document. Your use of the facilities must at all times comply with this policy and standard email security policies. Failure to adhere to this policy may result in a security breach or loss of NG data that could result in a disciplinary procedure.

If the device is a personal device, your line manager must approve and confirm that the requirement is compliant with the personal device security statement at the end of the document.

This document does not cover the use of personal devices to access National Grid email via an internet browser at https://webmail.nationalgrid.com. This Outlook Web Access (OWA) service is available as standard to all email users and can be accessed from any device.

Policies and Conditions for all devices

National Grid data stored on the device is subject to all National Grid policies and procedures. Therefore, National Grid will use a number of security features on the device to mitigate risk of data loss / theft. If you wish to use the service, you must not remove, disable, or bypass these controls, which include:

Strong Password (as per company policy)
Screen Lock Protection (the screen will lock after of a period of inactivity)
Remote Wipe Facilities (ability to delete all data remotely)
Encryption (data will be stored in an encrypted format)
No unsigned applications (applications can only be installed from official App stores)

In certain cases, it may be necessary for National Grid to have access to the device in order to install appropriate security software or analysis in the event of security incident.

Protection for our Data

National Grid retains the right to delete all data on the device, using the remote wipe facility if the device is lost, stolen, or for any other reason, to protect National Grid data. This will delete all personal data including **all private contacts, photos, videos, music, text messages, applications, purchased downloads and all other personal information that is stored on the device** as part of this process. It is therefore recommended that you take a regular backup of the device. It is a requirement that any backup is encrypted. Details of how do to this for iOS devices can be found here. (Please follow the instructions under iTunes). Please see your phone manual if you have a non-iOS device.

Cloud Restrictions

You are not allowed to synchronise National Grid data with iCloud or other cloud based solutions such as Google Sync, Dropbox, and Amazon Whispernet etc.

Device and OS Requirements

Only devices approved by National Grid can access National Grid services. Only devices running the official vendor sourced operating system are approved (i.e. the device cannot use "jailbreak" or other custom operating systems). You should ensure that all security updates from the device vendor are applied in a timely manner. It is expected that the device will generally be running the latest version of the operating system. National Grid may prevent specific operating systems versions from connecting to the service where this is deemed necessary. Once the service is enabled, you must not synchronise any other non-approved device. National Grid may change the list of authorised devices at any time, to add or remove devices from the list.

Approved personal devices are:

1) Android based devices running Android V5.0 and above (Lollipop and above)
2) Apple based devices running iOS 8 and above
3) Blackberry 10 or above devices
4) Windows Phone 8.1 Update 2 or above devices

In addition to the OS requirements Android devices must support device and storage card encryption, have Google Play store installed and have "Verify Apps" enabled (typically located under security settings).

Any personal device connected to the service must support and have device encryption enabled.

Lost, Stolen or Concerned

If the device is lost, stolen or you have any other security concerns, you must report the event immediately to National Grid security through the standard incident management process. As soon as practical initiate a remote wipe by accessing your email from any internet connected browser at https://webmail.nationalgrid.com and selecting options, followed by mobile phones, selecting device, and then selecting wipe device.

Device Software

Please ensure that all "personal software" on your device is correctly licensed. Any software provided by National Grid will be correctly licensed; however, personal software may not be licensed for business use. Should you have any questions about licensing of corporate software please contact the IS Service Desk.

Legal Hold and Leaving the Company

If you become subject to a legal hold notice you must not remove data relating to the legal hold notice from the device without the explicit permission of National Grid legal counsel. If you leave the company whilst under a legal hold notice, you must make available all data relating to the legal hold notice to National Grid prior to leaving.

Company Wi-Fi

Smartphones and tablet devices are not permitted to connect to or access the corporate network infrastructure directly including through Wifi or Ethernet access. The device may be used on corporate "Guest" Wifi networks subject to capacity availability and acceptance of T&Cs associated with the Guest Wi-Fi service. You are reminded that you are not allowed to connect other (non-smartphone / tablet) corporate devices to the "Guest" Wi-Fi networks.

SIM's

You must not put a corporate SIM card into a personal device.

Usage Monitoring

Monitoring of the usage and content of the corporate services provided will take place where, and to the extent that, National Grid is permitted to do so lawfully. All breaches, or suspected breaches, of the Information Security Management and Acceptable Use Policies must be reported. Any misuse or abuse of National Grid's data via a device will be taken seriously and may result in invocation of the disciplinary procedure and potential sanctions.

Costs

Not all email role profiles are entitled to use the EAS service (Task Based Worker, Field Worker, and Contingency Worker). If required, the employee will be moved to an appropriate role profile (Standard Knowledge Worker) in order to provide this service. This will incur an additional on-going cost to National Grid of between £20 / $40 and £60 / $120 per year. In addition to the cost, the employee will also gain a larger email account and full access to Lync Collaboration services.

Policies and Conditions for Corporate Owned Devices

Leaving the Company

If you leave National Grid, the device must be returned to your line manager (along with other IT equipment) in accordance with the Leavers Process. All National Grid data must be removed from any other device that you have synchronised backups to and your line manager should be informed when you have completed this by deleting the account profile and performing a factory reset of the device.

MDM Protection

Users that require access to company developed applications or MyServices will be provisioned on National Grids MDM. This service will provide enhanced services and security features. You will be required to make the device available (physically or remotely as appropriate) and to have the device reset to factory defaults if necessary.

Device Permission

The provision of a corporate phone does not give permission to connect a personal tablet to the service and vice versa. Any connection of a personal device is subject to line manager approval of the security declaration at the end of this document.

Personal Use Advice

The device should be used in accordance with the standard National Grid policy in relation to accessing illegal or other inappropriate material. While a degree of personal use of the device is allowed this should be limited, so as to not incur an increase in airtime or data costs. In particular, you should defer from using high bandwidth services such as audio and video streaming (Spotify, YouTube etc.) Personal use should not impact your ability to perform your duties or disadvantage National Grid in any other way.

The corporate device should not be used outside your country of residence unless approved by your line manager for work purposes. Charges for calls can be as much as 95p per minute and data can cost as much as £3 per Mb in certain countries.

The device should not be used to procure services and goods on behalf of National Grid. You should not make any purchases or subscribe to any services, which are billed to the airtime contract of the device whether directly, via SMS, premium rate services or any other method.

Policies and Conditions for personally owned devices

Privacy

National Grid cannot “view” any personal data on your device. National Grid can access some device parameters (such as operating system version), and can remotely set some configuration parameters (such as password settings). By using this service, you have granted National Grid the right to access this data and remotely set these parameters.

Leaving the Company

If you leave National Grid, or no longer wish to use your device to access National Grid data, then all National Grid data must be removed from your device and any other device that you have synchronised backups to and you should raise a request on IS to disable the email service on your device. Your line manager should be informed when you have completed this.

Job Change

If your job role changes, such that you no longer comply with the security declaration, you should terminate your use of the service as described in the previous paragraph (Leaving the Company). If you change line manager, your new line manager should be made aware of your use of the service to confirm continued use is appropriate.

Liability

National Grid is not held responsible for any damage, failure, or loss of your personal device or data contained on it, excluding any damage, failure, or loss caused directly by any wrongful or negligent act or omission of National Grid. Device support and configuration (hardware and software) are the sole responsibility of the end user excluding any remote settings by National Grid outlined above or business applications deployed by National Grid. National Grid will not reimburse you for any airtime charges incurred using this service.

Management Agreement for Use of this Service

As part of the terms of use of this service, you are required to get approval from your line manager to confirm your role is appropriate for the use of this service.

The statements below refer to the criteria your line managers needs to be aware of when approving your use of the service.

Personal Device

If through the normal course of their duties an employee receives data classified as Confidential, Highly Confidential, Legally Privileged or Price Sensitive then they are **NOT** a candidate for receipt of mail via ActiveSync on a personal device. If the employee does not normally receive data of this classification then you are able to grant them access to corporate email via ActiveSync on their personal devices if that device is on the approved list (as detailed above) and if that user reads and signs this Acceptable Usage Policy.

Please note that guidance on classification of data for assessment of the above criteria can be found in the following document ISMS 102 Protecting Information - Standard Guidelines

In the event the user role profile needs to be changed, you are also authorising the increased cost to National Grid and the increased functionality in ICE services provided by the change in user profile as detailed above.

Corporate Device

If there is a valid business reason why mail is needed while the employee is mobile then a standard corporate device should be provided. In the event the user role profile needs to be changed, you are

also authorising the increased cost to National Grid and the increased functionality in ICE services provided by the change in user profile as detailed above.