11 April 2024

Dear

**ATISN 20341**

Thank you for your request which was received on 12 March 2024. I have provided my response to each of the questions you submitted, at Annex 1.

If you are dissatisfied with the Welsh Government's handling of your request, you can ask for an internal review within 40 working days of the date of this response. Requests for an internal review should be addressed to the Welsh Government's Freedom of Information Officer at:

Information Rights Unit
Welsh Government
Cathays Park
Cardiff
CF10 3NQ
or e-mail: Freedom.ofinformation@gov.wales

Please remember to quote the ATISN reference number above.

You also have the right to complain to the Information Commissioner. The Information Commissioner can be contacted at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire, SK9 5AF

Telephone: 0303 123 1113
Website: www.ico.org.uk

However, please note that the Commissioner will not normally investigate a complaint until it has been through our own internal review process.
Yours sincerely

**Annex 1**

1. **Which Ministers use Whats App for the purpose of undertaking work associated with Welsh Government?**

   WhatsApp is not approved for use for Government business and is not installed on Welsh Government issued phones.

2. **Copies of current guidance on the use of IT (to include - phones which are personal and or Ministerial, laptop, desktop, tablet or other electronic communications device).**

   The information that follows is in scope of your request.

## Welsh Government Security Policy [v.5.8 – September 2023]

### *5. Protecting our ICT*

*You are responsible for taking care of the ICT equipment that you use and for safeguarding any login credentials, passwords or PINs that have been allocated to you.*

### *5.1 ICT Equipment*

*You are personally responsible for any ICT equipment allocated to you. Welsh Government maintains an audit trail of activity conducted on its network.*

*Welsh Government retains full remote access rights to all of the devices where its information is stored to maintain the security of those devices.*

*Laptops, smartphones and mobile devices should be switched on to receive automatic updates at least once every two weeks. Should you choose to retain your device whilst away for any long term reason e.g. whilst on parental leave then your device may require a long restart period or may need to be returned to IT Services for manual updates to be applied.*

*<u>You must:</u>*

*i. Never use your own ICT device for sharing or processing official business or attempting to connect to corporate documents;*

*ii. Immediately report any misplaced, lost, stolen or damaged equipment to the IT Service Desk;*

*iii. Always store ICT equipment e.g. laptops, iPads, cameras, mobiles and removable media in a secure location. See Section 7 for how to store paperwork and ICT equipment;*

*iv. Only attach devices to the corporate network or ICT equipment that have been approved through the IT Service Desk or those listed in Annex C;*

*v. Store passwords and PINs separately from ICT equipment (including shared equipment);*

*vi. Lock your computer screen whenever you leave your desk and also power down your laptop at the end of the day;*

*vii. Not allow anyone else e.g. a colleague to use your ICT equipment (laptop, smartphone, mobile phone etc) when you are not present;*

*viii. Not allow anyone else, e.g. a visitor, colleague, friend or family member to use your username/password;*

*ix. Not allow anyone without allocated Welsh Government equipment of their own e.g. contractor, friend, family member to use you ICT equipment (laptop, smartphone, mobile phone etc) even if you are present;*

*x. Change your password or PIN immediately if you suspect that it has become known to anyone else;*

*xi. Return corporately owned ICT equipment (raise a request on MyIT) when you no longer require them;*

*xii. Raise a MyIT request if you need any Welsh Government ICT equipment to be fixed e.g. printer, docking station, monitor, Tiny device to be moved etc.*

### *5.2 Email*

*<u>You must:</u>*

- *Only use Welsh Government ICT equipment and your Welsh Government email address to conduct official business.*

### *5.3 The Internet / Social Media*

*<u>You must:</u>*

- *use two factor authentication where it is available.*
- *Seek authorisation prior to downloading software from the internet*

### *5.4 Telephones (including smartphones and other mobile devices)*

*Like email, Welsh Government telephones are provided for the purpose of undertaking official business but may be used in an emergency. They are not a substitute for a personal device. Mobile numbers cannot be transferred to an individual when they leave the Welsh Government.*

*<u>You must:</u>*

*i. Use all available security devices such as keypad locking codes and PIN codes to prevent unauthorised use in the event of loss or theft;*

*ii. Not loan or transfer a smartphone or mobile device that has been issued to you to anyone else e.g. work colleague, contractor, friend or family member;*

*iii. Not allow anyone else e.g. a colleague to use your phone when you are not present;*

*iv. Not allow anyone without allocated Welsh Government equipment of their own e.g. contractor, friend, family member to use your phone even if you are present;*

*v. Seek approval for additional apps to be downloaded to your phone using MyIT. Requests for apps with no business relevance will not be approved.*

## *6. Personal Use of ICT Equipment – laptops, email, smartphones, phones, printers etc.*

*Welsh Government ICT equipment is provided primarily for official business. They are not a substitute for a personal device. The two exceptions to this rule are that:*

*i. ICT equipment can be used for personal use in the case of an emergency e.g. to deal with caring responsibilities that arise during work time.*

*ii. Limited internet browsing is permitted during non-working hours (e.g. lunch time and when travelling away on business).*

*All personal use of Welsh Government ICT equipment is carried out at your own risk. Welsh Government accepts no liability for any loss or damage arising from personal use of its ICT systems/equipment.*

*Any personal use of Welsh Government ICT equipment which affects the performance of the ICT systems or which has the potential to bring the organisation into disrepute could result in disciplinary action.*

## *Annex C – What personal devices can I connect to my laptop?*

*You must not attach ANY device to the corporate network or ICT equipment that has not been approved through the IT Service Desk. This includes charging personal mobile phones or tablets via the USB port on your laptop or docking station.*

*Removable devices, such as USB devices used for work related purposes, must be obtained through centrally agreed arrangements. Only Bluetooth headsets supporting Bluetooth 5.0 or above are permitted.*

*<u>Permitted personal devices</u>*

- *Monitors / TVs – either wired or wireless*
- *USB or Bluetooth mice, USB or Bluetooth keyboards*
- *Wired USB or Bluetooth Headsets - Only wired USB or Bluetooth headsets that support Bluetooth 5.0 or above are permitted. You must ensure that you have correctly paired the headsets directly to your laptop prior to use. If uncertain about pairing to the correct device, then you must remove and restart the pairing. IT Services are unable to offer support in connecting personally owned headsets, so please refer to your manufacturer's guidance if you experience any issues. Please note the exception that wireless headsets meeting DECT standards issued by IT Services as part of a reasonable adjustment are permitted.*
- *External cameras*
- *Printers: but ONLY if:*
    - *Your printer is Mopria certified; and*
    - *Your printer is connected to your laptop by a USB cable; and*
    - *You have a personally owned shredder that meets the P-4 standard (i.e. where the shredded particles are less than 6mm in width and the overall area is less than 160mm2) to shred OFFICIAL-SENSITIVE or personal information and mix the particles with normal household waste.*

*What personal devices can't I connect to my laptop?*

- *Wifi Headsets (only wired USB and Bluetooth headsets are permitted).*
- *USB / Bluetooth Smart Speakers including digital assistants like Amazon Echo and Google Nest.*
- *Electric cigarettes / Vapes: do not connect devices to your laptop to charge them. Use a 3 pin socket instead.*
- *USB novelty items such as Christmas lights, desk fans, cup warmers.*
- *Jigglers: These devices connect to your laptop and are designed to keep your screen active by randomly moving your mouse. They can also give the appearance that you are active on your laptop when you actually aren't (e.g. Teams status).*
- *Mobile phone: Do not charge your personal devices e.g. phone or tablet from your work laptop or docking station.*
- *Memory sticks / hard drives: While you have read-only access on your laptop, under no circumstance should you connect memory sticks / hard drives from unknown sources (e.g. found in the street or from trade shows) as these could be malicious. USB read access is only allowed for memory sticks / hard drives that have been approved for business use.*

## Ministers - Microsoft 365 and Mobile Devices [v2.0 - February 2024]

*Mobile devices e.g. phones and laptops are owned by the Welsh Government and are provided for business use. They are not a substitute for a personal device.*

***Use** – mobile devices and laptops are for your exclusive use. You may not loan or transfer them to anyone else e.g. a work colleague, contractor, friend or family member. You are responsible for all activity that takes place on the device and must not share your password or PIN with anyone else.*

***Lost / stolen** – if the device is lost or stolen you must immediately report it to your Private Office who will inform IT Services. IT Services may remotely wipe all information on the device if it is not in a safe location.*

***Overseas -** If you are travelling overseas, seek advice from the Departmental Security Unit before you travel with your device. Other countries do not have the same legal frameworks as in the UK and when overseas, your device will be subject to different cyber threats. These vary significantly depending on the country being visited.*

## Policy for Using Welsh Government Smart Devices that are not Configured for Welsh Government Email [v2.03 - September 2023]

### *1 INTRODUCTION*

*1.1 This policy sets out the appropriate standards of behaviour expected by everyone who uses a Welsh Government tablet (e.g. iPad, Android), camera or smart phone (e.g. iPhone) that is not configured to access Welsh Government email.*

*1.2 This policy is part of the Security Policy and so breaches of this policy may lead to disciplinary action as described in the Security Policy.*

*1.3 All devices are provided for work purposes. Limited personal use is permitted as described in the Security Policy (section 5 – Protecting Our ICT and section 6 - Personal Use of ICT Equipment – laptops, email, smartphones, phones, printers etc.).*

*1.4 You may be asked at any time by your line manager to immediately return the device. You may not be given any time to retrieve any personal files from the device. It is your responsibility to back the device up at regular intervals on your own equipment if you wish to retain copies of any personal files.*

### 2 CAMERAS

*2.1 Cameras must only be used for work related purposes. They must not be used for personal use.*

*2.2 As pictures taken with cameras are potentially in scope for Freedom of Information requests, the pictures must be transferred to the corporate network as soon as possible and then deleted from the camera. The pictures must then be managed in accordance with the Welsh Government's Information and Records Management policy, in the same way as any other information that is created for work related purposes.*

*2.3 Pictures must not be stored in personal storage areas e.g. iShare Home folder or e-mail folders.*

***3. TABLETS AND SMART PHONES** (jointly referred to as 'device' or 'devices' for the remainder of this policy)*

*<u>You must:</u>*

*i. Add all devices to the asset register. If you purchased the device via the IT Service Catalogue, then the device will be asset tagged before it is given to you. You must obtain an asset tag from IT Services for any device purchased outside this arrangement;*

*ii. Only use the device to access the Welsh Government's network via the appropriate methods as outlined in the Security Policy. If required to do so, register the device using a personal credit card. A Welsh Government procurement card must not be used to register the device. If you share the device with other members of Welsh Government staff, you must sign out of the device so that your details are inaccessible;*

*iii. Activate all security/PIN codes. If you have to write the PIN code down as a memory aid it must be written on a blank sheet of paper giving no indication of what it relates to and not stored with the device;*

*iv. Activate any available apps that allow you to remotely locate the device if it is lost/stolen e.g. Find My iPhone app which is designed for iPads, iPhone and iPod Touch devices;*

*v. Immediately report any loss or damage to the device to the IT Service Desk. If the device includes any 3G/4G/SIM capability you must also immediately report it to the network provider e.g. EE, Vodafone;*

*vi. Contact IT Services via MyIT to have the device formally re-allocated to another member of staff if you no longer have need of it. You must not pass the device on to another member of staff on a permanent basis unless it is formally allocated to them. Whilst the device is formally allocated to you, you are responsible for it. If you loan the device to another member of staff you must keep a record of the loan;*

*vii. Store the device securely as detailed in the Security Policy e.g. if left in the office it must be locked away overnight, not left unattended or left in a vehicle overnight;*

*viii. Take care of the device to prevent any avoidable damage e.g. ensure that it is fitted with a protective case/cover;*

*ix. Ensure that all personal use of the device is compliant with the Security Policy. For example:*

- *downloading a major national newspaper is acceptable but accessing a website that advocates hate/violence is not;*

- *accessing your personal email is acceptable provided that you do not use your personal email account for business.*

*You must not (list not exhaustive):*

*i. Allow someone who is not a Welsh Government member of staff to use the device;*

*ii. Store any business information on the device. If you use the camera functionality to take a picture for business purposes, it must be emailed into the network as soon as possible and deleted from the device. The pictures must then be managed in accordance with the Welsh Government's Information and Records Management policy, in the same way as any other information that is created for work related purposes. All other business information must only be accessed via the Stratus service;*

*iii. Use personal email or any other facility e.g. Dropbox to conduct Welsh Government business unless you have written authorisation from your Information Asset Owner;*

*iv. Access any app or website that could bring the Welsh Government in to disrepute. If any activity/website is not permitted from the Welsh Government's corporate network, it is unlikely to be suitable for access from any Welsh Government device;*

*v. Subvert any manufacturer's control e.g. jailbreak an Apple device to allow you to use apps that have not come from the Apple store. Whilst jailbreaking a device (known as rooting on Android) is not illegal, it is not acceptable for Welsh Government devices;*

*vi. Reset the device to factory settings to hide any activity that you have undertaken on the device which is in breach of this policy.*

## Guide to Working / Travelling Overseas [July 2022]

### *3.0 Using ICT Equipment Overseas*

*If approval has been granted to take your ICT equipment overseas, then you must:*

*i. Check that your work phone is updated to the latest iOS and also ensure your laptop has the latest security patches/updates installed before travel. The IT Service Desk can help advise if necessary;*

*ii. If travelling for business reasons, enable international roaming by completing the relevant form on MyIT if taking a mobile phone, or other data-enabled device overseas for the first time for business reasons (see instructions below);*

*Note: if you are travelling for personal reasons, the cost of any data charge is a personal cost and will not be met by Welsh Government;*

*iii. Alert the IT Service Desk as soon as possible if your device is lost or stolen;*

*iv. Report all instances of loss/theft to the local police so that a crime/incident number can be obtained;*

*v. Carry all ICT equipment in your hand luggage unless for security reasons this is not permissible;*

*vi. Inform the Departmental Security Unit if you have had to divulge your password as a condition of entry to your destination country. You must also change the password as soon as it is safe to do so;*

*vii. Contact the Departmental Security Unit if ICT equipment has been out of your care before you reconnect the equipment (either directly or remotely) to the corporate network;*

*viii. Be aware that Global Protect on your laptop may not work from the country that you are visiting and you may not have access to certain facilities (e.g. iShare, MyIT);*

*ix. Consider how you will access files in such instances before you travel e.g. consider the temporary use of OneDrive or Objective Connect to access documents.*

***International Roaming***

*If you are travelling for business reasons and are unsure whether your device is already set up for international roaming, contact your network provider, who will also be able to offer advice on the kind of service you can expect while you are abroad.*

*If you have permission to take your mobile equipment overseas for business reasons and you turn on data roaming, you could generate a significant bill. Keep data use to the absolute minimum and use wifi where possible. If data use overseas is essential, speak to IT Services in advance so that they can advise you of data limits and costs.*

*Note: putting in a request for international roaming is not a request for authorisation to take ICT equipment abroad. International roaming will not be actioned until the Departmental Security Unit have authorised your travel plans.*

## 3. Copies of previous version over the past 5 years.

The information that follows is in scope of your request.

### Welsh Government Security Policy

30 September 2022 – version 5.6

*Change to Annex C – staff can no longer charge their personally owned IT devices (mobile phones, tablets) from their work laptop*

06 April 2022 – version 5.4

*Change to Annex C - Bluetooth headsets version 5.0 and above may be connected to a work laptop.*

27 September 2021 – version 5.2

*Change to Annex C – personal printers can now be connected to a work laptop in some circumstances*

13 January 2021 – version 5.0

***5.1 ICT Equipment***

*You must:*

*iv) Not attach any device to the corporate network or ICT equipment that has not been approved through the ICT Service Desk e.g. do not connect unauthorised or personal USB, wireless or Bluetooth devices to laptops or docks See Annex C for further information*

***Annex C - What personal devices can I connect to my laptop?***

*You must not attach ANY device to the corporate network or ICT equipment that has not been approved through the ICT Service Desk. This includes charging personal mobile phones or tablets via a USB port except in an emergency (e.g. you are travelling for work and do not have a 3 point charger and your phone is low on charge).*

*Do not connect unauthorised or personal USB, wireless or Bluetooth headphones to laptops or docks. Only wireless headsets meeting DECT standards issued by ICT Services as part of a reasonable adjustment are permitted.*

*Permitted personal devices*

- *USB Wired Headsets - Only wireless headsets meeting DECT standards issued by ICT Services as part of a reasonable adjustment are permitted.*

*What personal devices can't I connect to my laptop?*

- *Wifi and Bluetooth Headsets (wired headsets* only are permitted)*
- *Jigglers: (e.g. Skype status).*
- *Printers: Under no circumstance should you connect your laptop to a personal printer, either wired or remotely. Only official homeworkers are allowed to print from home.*
- *Mobile phone: Only charge your work phone in an emergency if a 3 pin plug isn't available. You may not charge any other items from your work laptops. Personal mobile phones must not be connected to laptops or docks.*

## Ministers - Microsoft 365 and Mobile Devices

24 Jan 2024 – version 1.2.1
***Overseas -** If you are travelling overseas, seek advice from the Departmental Security Unit before you travel with your device*
Also contained information on personal use. Removed in current version (February 2024):
*Whilst primarily provided for business use, you can make reasonable personal use of the device e.g. phone calls, photographs and access to your personal email. However, please note the following:*

- *The associated telephone number belongs to Welsh Government and will not be transferred to you at a later date;*
- *The telephone number must not be registered for any personal use e.g. you must not register it as a device associated with your internet banking account;*
- *Personal use e.g. social media, internet or email access counts towards your data tariff so you may wish to limit personal use to when you have a Wi-Fi connection;*
- *You must not mix business and personal information e.g. the Outlook app is to be solely used for Welsh Government email. You must not register any other app for Welsh Government email or add any other account to the Outlook app;*
- *Welsh Government is not responsible for maintaining access to the device for personal reasons e.g. if the device needs to be wiped in order to fix it, engineers will not take a copy of your photos first, all information will be removed, possibly without notice.*

21 Sep 2022 – version 2.1
***Overseas** – if you are travelling anywhere other than North America or Europe, please seek advice from the Departmental Security Unit before you travel with your device.*

## Policy for Using Welsh Government Smart Devices that are not Configured for Welsh Government Email

Previous versions stated that it was permissible to take personal photographs. Removed in current version (April 2021). No other relevant changes.

## Guide to Working / Travelling Overseas [April 2020]

***Using ICT Equipment Overseas***
*<u>You must:</u>*
*i. Seek authorisation from the Departmental Security Unit to take ICT equipment to any country that is not on the 'approved' list overleaf. This includes stop-over countries as well as your final destination;*
*ii. Ensure that your Line Manager is content with your travel arrangements before seeking security authorisation, especially if you are planning to use ICT equipment whilst you are on annual leave;*
*iii. Check that your Smartphone is updated to the latest iOS and also ensure your laptop has the latest security patches/updates installed before travel. The ICT Service Desk can help advise if necessary;*
*iv. Enable international roaming by completing the relevant form on MyIT if taking a mobile phone, Smartphone or other data-enabled device overseas for the first time;*
*v. Alert the ICT Service Desk as soon as possible if your device is lost or stolen. For mobile phones or Smartphones you must also contact your network provider (Orange (EE), 150 from an EE phone, 07953 966 250 from any other phone (at standard rates) or +44 7953 966 250 from abroad (at international call rates) or the Vodafone 24-hour Lost and Stolen helpline (+44 7836 191 191) – free from any Vodafone phone even while you're abroad (international call charges apply from any other mobile or landline) immediately so that they can place a bar on the sim;*
*vi. Report all instances of loss/theft to the local police so that a crime/incident number can be obtained;*
*vii. Carry all ICT equipment as hand luggage unless for security reasons this is not permissible;*
*viii. Inform the Departmental Security Unit if you have had to divulge your password as a condition of entry to your destination country. You must also change the password as soon as it is safe to do so;*
*ix. Contact the Departmental Security Unit if ICT equipment has been out of your care before you reconnect the equipment (either directly or remotely) to the corporate network.*

| ***APPROVED LIST OF COUNTRIES*** | | | |
|---|---|---|---|
| *Australia* | *Austria* | *Belgium* | *British Isles* |
| *Bulgaria* | *Canada* | *Cyprus* | *Czech Republic* |
| *Denmark* | *Estonia* | *Finland* | *France* |
| *Germany* | *Greece* | *Hungary* | *Iceland* |
| *Republic of Ireland* | *Italy* | *Latvia* | *Liechtenstein* |
| *Lithuania* | *Luxembourg* | *Malta* | *New Zealand* |
| *The Netherlands* | *Norway* | *Poland* | *Portugal* |
| *Romania* | *Slovakia* | *Slovenia* | *Spain* |
| *Sweden* | *Switzerland* | *USA* | |

***International Roaming***
*If you are unsure whether your device is already set up for international roaming, contact your network provider, who will also be able to offer advice on the kind of service you can expect while you are abroad.*
*Note: If your destination (or stop-over) country is not one of those listed above, your request for international roaming will not be actioned until the Departmental Security Unit have authorised your travel plans.*

4. **Any information, instructions etc provided by the Senedd ICT department on the methods of cleansing data from any of the above.**

Senedd Cymru is a separate organisation to Welsh Government – we therefore do not hold this information.  Details on how to make requests to Senedd Cymru can be found here Freedom of Information (senedd.wales)

5. **Details of the number of FOIs and dates in which information has been sought around the deletion of any data files, messages etc in the past 5 years.**

   Welsh Government reference ATISN 20133 – received 21 Jan 2024; and
   Welsh Government reference ATISN 20317 – received 5 Mar 2024

6. **Copy of the protocols that are in place if a Minister steps down from their role to ensure any data files from any source are secured.**

   The information requested is exempt under Section 21 of the Freedom of Information Act (2000) – information reasonably accessible to the requester by other means. The Information Management & Governance Policy is published on the Welsh Government website. Welsh Government follows the National Archives Guidance on the Management of Information in Private Offices which is also publicly available.