Working With Portable Technology and Documents Procedure

This procedure is part of North Yorkshire Police policy to which all Chief Constable personnel and the functions provided by the Deputy Mayor for Policing as part of the York & North Yorkshire Combined Authority are required to adhere.

Procedure Statement

North Yorkshire Police (FORCE) allows staff to work from police premises or other non police locations using FORCE documentation and authorised equipment such as mobile devices.

This procedure applies to, but is not limited to, the following:

- Laptops;
- Any electronic storage mediums i.e USB memory stick, CDs, DVDs;
- Mobile / Smartphones;
- Tablets(iPad etc);
- Audio/video;
- Documents and files (including photographs).

Purpose

The purpose of this procedure is to provide the general requirements of the use of devices, the transfer of information and the specific instruction when using FORCE information or equipment.

Aim

To ensure the security of FORCE information assets regardless of the location from where police business is being carried out.

Objectives

The procedure objectives are:

- to provide clarity to those activities which are deemed to be strictly forbidden;
- to detail the criteria for the allocation of equipment;
- to detail the requirements of all staff using any device or documents;

- to provide clarity for the use of FORCE data in public places;
- to provide guidance for staff arranging presentations etc from outside agencies/other forces;
- to provide guidance in relation to the use ABROAD of devices;
- to provide clarity in the event of compromise (what to do);
- to provide guidance on wireless connectivity;

Overarching Policies:
Information Security

Procedures:
Internet and e-mail Procedure
Security Incident Reporting Procedure
Security Incident Handling Procedure
Data Protection Procedure
Protective Marking Procedure
Clear Desk and Clear Screen Procedure
Physical Security Procedure

Other Documents:
Data Protection Act 1998
HMG Security Policy Framework
ICT Removable Media Subsite
Secure Communications Guidance

Process

This procedure covers the FORCE requirements for all staff and officers, including volunteers, relating to the use of laptop computers, mobile devices and FORCE documents, whether on FORCE premises, partnership locations, working from home or abroad or using FORCE on premise systems or cloud based systems.

All custodians of devices or documents must comply with relevant PSD and ICT procedures as well as the security advice contained within this procedure.

The use of a FORCE laptop computer or other mobile device is defined as any portable device that has the ability to store, process or transmit information by electronic means such as mobile data terminal, storage medium and mobile/smartphones.

The transmission, import and export of data can include the copying of force data onto discs to use elsewhere, the use of home computers for work purposes and e-mailing of work to and from personal e-mail accounts.

FORCE documentation can include computer printouts, case files, photographs, memos, reports, notes etc.

In all cases it should be noted that the following activities are **STRICTLY FORBIDDEN:**

- conducting FORCE work on a home computer or other private computer or device unless appropriate authority has been given and all security safeguards are in place;
- E-mailing FORCE data to a personal e-mail account unless for an authorised policing purpose;
- the processing, storage, retention or disposal of FORCE OFFICIAL information or that of a FORCE partner for a none policing purpose;
- The sharing of FORCE data or that of a partner through non-secure means (electronic or hard copy) and without the authority of a contractual agreement, Information Sharing Agreement or Data Processing Contract in place which authorises such transmission or you have a justifiable policing purpose to do so and an auditable trail which will stand to scrutiny. See the section entitled "Secure e-mail addresses" below and read the Secure Communications guidance;
- downloading of any data onto removable media device or storage medium unless approved and issued from ICT stock and for an authorised policing purpose;
- any connection from a laptop or mobile device to any unauthorised network or system whether that be wireless or hard connection. Further information can be found in the wireless connection section;
- the use of devices which are not owned and supported by the force e.g. mobile/smartphones, storage mediums, laptops, tablets, headsets etc. Such devices are prohibited from use due to the security threat that they pose as they will not be subject to the same technical security afforded to authorised FORCE devices. Unless the removable media is authorised by FORCE, it will not be able to connect to any FORCE computer equipment;
- Using FORCE devices/hardware for non-policing purposes such as printing personal documentation.

Allocation of Equipment

- ALL laptops and other mobile devices issued by ICT must be approved and signed for at the time of issue. The order process for devices can be found here – RM01 – Request for Removable Media;
- ICT equipment is issued to the role as opposed to the individual and should be returned to ICT for re-configuration and re-issue in the event of the custodian leaving their role. This includes any laptop, tablet, smartphone or storage medium. The procedure for returning a device can be found here – Return of ICT Issued Equipment;
- no other person must be given access to the equipment other than the authorised custodian. ALL FORCE staff and officers, including volunteers, must comply with existing policies regarding not sharing passwords or allowing others to use one's log-on session on any device type.

Requirements of all Staff Using any Device or Documents

The following instructions must be followed at all times but are particularly important when working away from force locations including home working and partnership premises.

- staff must ensure they have a working environment of equivalent comfort, safety and security to that afforded at their place of work;

- when in transit, all hardware or documentation must be kept in the personal possession of the custodian. All reasonable steps must be taken to ensure that no compromise of the device or material can take place;
- when not in use, all hardware or documentation must be kept in a secure location and the custodian must be aware of its whereabouts at all times. Equipment and documents should be checked for any signs of tampering. **Please note: an unattended vehicle is not considered to be secure;**
- Users are encouraged to digitise their official work and tasking as much as possible. If you are in a role whereby you have justification to handle sensitive hard copy Policing data outside of secure policing premises i.e. at home, it may be necessary to have secure storage available. All cases are to be registered with the Information Security Officer and you should contact the Information Security Team to discuss your requirements;
- the electronic device or documentation must only be used for authorised policing purpose(s);
- no sensitive material with a Government Security Classification marking of Official Sensitive or above must be stored on the laptop or mobile device without the consent of the Information Security Officer. Such consent will only be given in exceptional circumstances;
- laptops/tablets must be switched off and the user(s) logged off when not in use. Do not leave laptops in 'hibernate' mode;
- laptops, tablets and smartphones must be connected to the network at least monthly to ensure all relevant security measures are adhered to and to allow firmware and software updates to take place e.g. Anti Virus. This will also allow your files to be synchronised and backed up. This action safeguards your work and maintains the security of the FORCE network;
- no other software or devices e.g. non authorised storage mediums, may be connected or inserted into (or installed onto) a FORCE computer, laptop or mobile device without ICT authorisation. Unauthorised software or devices may contain viruses which will corrupt the FORCE network and will be traced to your device;
- user(s) must not attempt to modify or alter any of the settings on a device. Such actions must only be carried out by an authorised administrator within ICT. Device settings are there to protect you against a breach of procedure or legislation and the FORCE network from viruses or other malicious attacks;
- no data must be transferred from the laptop, tablet or mobile device to another device unless it is for an authorised policing purpose and has the permission of the Information Security Officer and ICT;
- where applicable, all authorised devices using wireless communication must utilise suitable encryption to ensure the security of the data whilst in transit;
- Smart devices with biometric authentication such as fingerprint and facial recognition may be used to promptly access the smart device for convenience. It is the users' own choice whether to use the technology. Users must remain cautious when using such technology as on occasion, authentication may fail due to angle of finger or face wear. In such cases after three attempts, users will then need to use alternative authentication methods such as fingerprint or password. Users will still need to provide the device nine-digit password if the device has not been authenticated for 24 hours. Users must remain vigilant in using such technology and asked to consider their surroundings and the safety and security of themselves and the

device when considering using the technology. Any security incident must be reported as per the Security Incident Procedure.

Use in Public Places

- staff with access to FORCE assets eg paper or electronic (such as Ironkeys), outside force locations should be discreet and not publicise the fact to anyone else. This is particularly important in shared households if working from home;
- care must be taken with the laptop, mobile device or paper documents to prevent anyone overlooking or eavesdropping on data while in public areas eg on public transport or within a shared office space outside FORCE premises;
- whilst this relates primarily to FORCE documents and devices, these principles should also be applied to other force or agency documents and devices.

Visitor and/or Other Agency Guidance

FORCE visitorswho wish to use removable media for presentations or meetings etc must comply with the following:

- e-mail their presentation to the visit organiser. If this is not possible, they must ensure the device is checked for viruses prior to using in FORCE equipment. This can be achieved quickly and simply by contacting ICT Service Desk for advice;
- where a FORCE staff member or officer wishes to process force data on a computer or system owned by another agency, the force Information Security Officer and ICT must authorise the proposal, ensuring there is both adequate IT and physical security.

Secure e-mail Addresses

The police and other criminal justice agencies use the PSNP and other secure networks, which permits the exchange of information up to and including the Government Security Classification of "Official Sensitive".

An email sent from one '.police.uk' email address to another '.police.uk' email address will remain within the confines of the PSN network.

There are other secure email addresses i.e. CJIT, CJSM. They exist in order to send and receive information via these networks, but users must ensure that the network they are using is a secure one if sending 'Official Sensitive' material.

Many person(s) within FORCE will be familiar in using secure connections such as GCSX and sending emails to domains as part of the GSI-family. The Governmental Digital Services (GDS) removed support for GCSX at the end of March 2019. Partners using a domain ending 'gov.uk' are enforcing encryption between the 'northyorkshire.police.uk' and their domain. All types of 'official' information can be sent to partners within North Yorkshire; namely Selby, North Yorkshire County Council, Harrogate, Craven, Scarborough, Ryedale, York, Richmond, Hambleton, Veritau.co.uk and the CPS (cps.gov.uk) without any additional encryption. However, please ensure you verify the email

account of the recipient Prior to sending. If you are looking to send 'official-sensitive' data to a local partner, further risk mitigation methods will need to be applied. Please refer to the Secure Communications Guidance.

If you communicate with a local authority or governmental partners (not using a pnn.police.uk domain) who are not listed above and you are regularly sharing 'official' and above information, please inform the Information Security Team so bespoke arrangements can be made with that partner to ensure they meet the GDS new standard. You can contact the team by emailing informationsecurity@northyorkshire.police.uk.

Information processed outside the PSN and other trusted networks may not necessarily be subject to the same security measures, therefore, the processing (by email transmission) of FORCE information or that of a force partner is strictly forbidden unless there is an Information Sharing Agreement or Data Processing Contract in place which authorises such transmission or you have a justifiable policing purpose to do so and an auditable record which will stand to scrutiny.

Microsoft Office 365

NYP users will be using Microsoft Office 365 and the exchange online service from early 2020 and full rollout will take place throughout the year. Users will not notice a significant difference in using exchange online and in other technologies as the interfaces are similar to what users are familiar with. However, users email domain will change from '@northyorkshire.pnn.police.uk' to '@northyorkshire.police.uk'. Other Police Services will also be changing their domain name, as will many partnering agencies i.e. '@york.gov.uk' as they all move to use Microsoft Office 365, all North Yorkshire local authorities use this solution. This means that official communications will be over the internet.

Sending emails from '@northyorkshire.police.uk' to another Police Service (@PoliceService.police.uk) or partner i.e. '@york.gov.uk' using Microsoft Office 365, is deemed secure for all official communications.

If an NYP user assesses communication to be official sensitive and/or requires further security protection, Microsoft's Information Rights Management provides further security protections including Office Message Encryption (OME), ability for the recipient to have limited time to access the document, the ability to restrict printing and editing rights the document. When sending an email, file or document which requires additional security, the recipient will need Azure Protect Viewer or a compatible application or software to access, view and amend it.

If you communicate with a local authority or governmental partner (not using Microsoft Office 365 and exchange online) and you are regularly sharing official and above information, please inform the Information Security Team so bespoke arrangements can be made with that partner to ensure they meet the GDS new standard. You can contact the team by emailing informationsecurity@northyorkshire.police.uk

Information processed outside the Microsoft 365 environment may not necessarily be subject to the same security measures, therefore, the processing (by email transmission) of FORCE information or

that of a force partner is strictly forbidden unless there is contractual arrangements, an Information Sharing Agreement or Data Processing Contract in place which authorises such transmission or you have a justifiable policing purpose to do so and an auditable record which will stand to scrutiny.

It is the users' responsibility to ensure they choose the appropriate level of security and communication type to transfer Police information to match the level of sensitivity in the information. Before sending ANY communications, please self-assess 'WHAT' information you are sending, to 'WHO', 'HOW' and 'DO' you require more security measures before sending?

If you receive an email intended for another person, please ensure you report the incident as per the Security Incident Procedure. You must delete any emails received in error and must not disseminate or sue the information further.

Before you send a message, make sure the addressees are approved to receive the information contained in or attached to the email. Care must be taken when using email copy (cc), blind copy (bcc) and reply to all functions to avoid confidential information being sent to other recipients in error.

Only FORCE email addresses must be used to send official Police emails, personal email addresses must not be used for this purpose.

Use of Laptops or Mobile Devices Whilst Abroad

Due to varying legislation in different countries regarding the use of portable media (e.g. the possibility of confiscation of any device in your possession) it is important to assess the situation prior to travel.

It is also important to assess the risk in connecting with overseas communications links and networks which may be more vulnerable to interception than those in the UK.

Taking and using equipment overseas can be complex and consideration will be given to cases in exceptional circumstances but it is in breach of NYP policy and in contravention of NYP accreditation to national policing systems to take and/or use NYP devices abroad without gaining the approval of the NYP information Security Officer and/or SIRO (DCC). Any attempt to access an NYP device from an overseas location will be spotted and blocked by our firewall and access will be revoked immediately from that device.

If an employee feels that such a request is deemed exceptional, then they should closely adhere to the following;

- what is the business requirement for taking/using the item overseas?
- when, where and how the device will be used?
- what, if any, are the actual or potential physical threats with the hotel/venue to be visited?
- consider other issues associated with using the item in a public place overseas – overlooking, theft, social engineering, interception of communications etc.
- what to do in the event of a security breach?
- does the item have encryption and, if so, to what level?

- does the communications infrastructure or technology required to support the item exist in the country to be visited?
- what is the current or potential threat within the country to be visited?

Advice on this can be sought from the Information Security Officer or ICT to assist an individual to undertake this assessment. Authorisation via email must be sought from the following including details of the destination, dates and nature of business:

- Line Manager
- Information Security Officer through to the Senior Information Risk Owner (if necessary)
- ICT

Compromise of Equipment/Documentation

If you believe your laptop or mobile device has been compromised in any of the following ways you must report this to the ICT Service Desk during office hours. Outside these hours, report it to the FCR. In addition, a Security Incident form must be completed (accessed via the intranet home page) and submitted to the force Information Security Officer. This applies to incidents such as:

- virus infection
- introduction of other malicious software
- use by an unauthorised party
- loss or theft of a laptop or mobile device

If ICT detect a virus you will be contacted and must comply with the instructions given.

If any FORCE documentation has been compromised in any way eg lost or stolen, you must inform the Information Security Officer by completing a Security Incident Report.

Wireless Connectivity:

<u>WiFi and MiFi</u>

What is an authorised network that can be used?

- FORCE corporate WiFi
- A FORCE employees' home network as provided by their Internet Service Provider (ISP) such as British Telecommunications, Sky or Virgin Media.
- Employees' personal MiFi or smartphone connection, if ISP broadband services are not available
- FORCE Smartphone tethering
- Partnership agency connection
- Member of the public's or businesses WiFi

The FORCE user is responsible for verifying the networks legitimacy by ensuring it meets some minimal standards. The user must identify and be satisfied with the host of the network i.e. City of

York Council and that the host is genuine and consent to connect is provided. Secondly, the network name (Service Set Identifier (SSID) is correct as broadcasted by the host. Thirdly the authentication process must be configured to a minimum of WPA2 (with password protection) before connecting to the network. Cyber threats such as rogue WiFi networks in public places do exist seeking to mirror genuine WiFi connections.

By default, the majority of domestic routers, portable connections such as MiFis and smartphone tethering do meet this authentication requirement. For any network connection made, the user must make a secure Virtual Private Network (VPN) connection through Blackberry connectivity, endpoint security or alternative remote access software provided by FORCE before carrying out any official FORCE network usage on your FORCE smartphone, tablet or laptop.

On completion of the visit or connection usage, the user(s) should evidence to the host that they have disconnected from the Wi-Fi prior to leaving the location.

What is an unauthorised network that can't be used?

- USB internet dongles that have not been issued by FORCE. These dongles require physical connection with a laptop, tablet or computer.
- WiFi connections through captive portals. These often require user(s) to enter log in details before connecting. User's interaction (agreeing to terms and conditions or entering a passcode) is required before an internet connection is allowed. These will be often found in hotels and cafes. These networks require mobile devices to browse to a website outside of a Virtual Private Network (VPN) connection; during this time devices can be targeted for attack by the network itself, or by hostile user(s) on that network. Configuring devices to enable this type of connection requires a mechanism to disable or circumvent the VPN, increasing the risk of compromise of data in transit.

Whilst in FORCE premises

When inside FORCE premises, laptops and tablets will connect through FORCE Wi-Fi to the Corporate Wi-Fi. This is the preferred connection for business usage. Smartphones will not automatically connect to the corporate WiFi. Smartphones and some tablets with SIM card access will utilise the Vodafone cellular network.

At a member of the public's home address or business

When an operational user(s) is at a member of the public's home address or business premises and requires a Wi-Fi connection, user(s) must follow the points under the authorised network heading.

FORCE smartphones tethering

FORCE smartphones may be used to tether a connection to a tablet or laptop if required. Only FORCE hardware will be connected to a FORCE smartphone tethered connection. A user must ensure they connect to the correct network, following the authentication process on the smartphone using the security features provided. The tethered connection must not be shared with non-FORCE hardware or person(s). Please note only the Samsung J5 (2016 / 2017) and J6 will have this feature.

Partnering agency connection

When the user(s) is within a partner agency building with Wi-Fi available, e.g. hospitals, council, probation offices etc, once connected, user(s) must make a secure VPN connection through checkpoint endpoint or any alternative remote access software FORCE provide. Once a secure connection has been established, all traffic must go through this connection. User(s) should not assume Council guest Wi-Fi is set up in this manner and should always check with the council first.

Public hotspots

Other Wi-Fi connections will be available, however connections in public places such as coffee shops, hotels and shopping centres are generally 'captive portals' and deemed as not secure. At all times user(s) should follow the existing rules within the Internet and Email procedure.

Bluetooth

Bluetooth provides a low cost, low complexity solution for short range wireless connectivity between a small handheld device and associated peripherals, often referred to as a Personal Area Network. NYP has a limited number of use cases for Bluetooth. All requests to use Bluetooth connectivity must be with prior approval and registered with the Information Security Officer.

Use cases approved include:

- Pairing with FORCE vehicles to talk over the Infotainment system
- Pairing with computer peripherals such as NYP issued wireless mouse / keyboard to support medical requirements and comfort.
- Pairing with NYP presentation training aids.

Terms of usage

- The device should only be paired or connected to another approved FORCE Bluetooth device or system, for example in-car equipment currently fitted in FORCE vehicles. All Bluetooth pairing must have a supporting policing purpose or supporting medical evidence.
- When the user(s) is required to undertake the pairing process of the device to another device or system, this should only be carried out in police secure premises or in a police vehicle.
- The device must never be connected to the user(s) own personal devices.
- Device's Bluetooth is to be turned off when not in use so the device is not discoverable.
- Any connections made to FORCE assets will be authenticated through use of a PIN and all connected devices will be trusted devices only.
- User(s) must, where possible, not use the connectivity in public and user(s) must be vigilant and cautious in its use. Any requests to pair will be rejected in public.
- No sensitive conversations are to take place over Bluetooth connectivity.
- Bluetooth usage is not suitable for covert use.
- Bluetooth is not suitable for sharing an internet connection. Please consider using smartphone tethering.
- Any loss, theft or damage to a Bluetooth device must be reported to ICT. In the case of loss or theft, the information security team are to be informed.

Responsibilities

Operational Officers/Police Staff

Are to be familiar with the Portable Technology and Documents Procedure and should act accordingly to protect the security of FORCE information and equipment either on or off FORCE premises.

First Line Supervision

Are to ensure their staff are aware of, and adhere to, the Portable Technology and Documents Procedure. In addition, supervisors must report any incidents arising from the non-adherence to this procedure.

Safer Neighbourhood Commanders

To ensure the continuing security of FORCE information and equipment and that any breaches of security are recorded and managed in an effective risk based manner.

Heads of Department/Function

To ensure the continuing security of FORCE information and equipment and that any breaches of security are recorded and managed in an effective risk based manner.

To authorise (or not, as the case may be) transmission by email outside of the CJX network.

Command Team

Overall responsibility for the security of all FORCE information and equipment.

Definition of Special Terms

CJX Criminal Justice Xtranet

.cjit Criminal Justice IT

.cjsm Criminal Justice Secure Mail