



Internet and Email Procedure

This document 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

We recognise that the use of the internet and email is an important tool in enabling you to undertake your role. We also recognise that while you are at work there are times when personal use is helpful.

Therefore, our general approach is to allow access to the internet unless there is a compelling reason to restrict access. Please use these tools with regard to the process points below and in the overall spirit of the Code of Ethics.

Linkages

Communications Policy
Secure Communications Guidance
Social Media Policy

Procedure

1) General

Individuals have access to internet browsing and email, both internally on the FORCE network and externally, via the intranet and cloud services in order to support your work, to access employee benefits and for personal use.

We do recognise that your personal lives don't stop when you are at work and that it is sometimes beneficial for you to use the internet for personal reasons (e.g. manage your personal accounts, make appointments or even do your food shopping online). All we ask is that you do not spend excessive amounts of time on personal activity and that all your online activity is in accordance with your commitment to the Code of Ethics. Please note that **all** activity on NYP hardware (laptops, computers, tablets) will be captured within the digital auditing software, namely ATA. The privacy notice can be found at Internal Monitoring and Auditing Privacy Notice.

Please bear in mind overall that we are a transparent public service. The content of FORCE email accounts and internet use is subject to the Freedom of Information Act (2000) and all responses to



Freedom of Information requests are published on the internet. Equally we are subject to the Data Protection Act so please take care on data security.

As internet and email traffic has a cost to us in usage, as does storage for both on premises and in the Microsoft Office 365 cloud environments, you are asked to limit use and delete files and content – only retain emails when it is necessary and proportional to do so. This will assist our overall efficiency.

Some internet content will be blocked. This could be because unblocking it will have an adverse impact on the ability of our systems to operate. For example, live streaming (e.g. YouTube) slows down our systems and could halt use altogether. Once we have implemented a range of IT developments, we may be able to revisit this. Content deemed inappropriate (pornography, gambling etc.) will be blocked.

Our basic rules and ways of working are that

- Individuals don't view material which is illegal, offensive, or sexual in nature;
- Individuals don't use systems to solicit business for profit or gain or to promote a business interest;
- Individuals don't represent personal opinions as those of FORCE or create or maintain personal blogs, websites or e-mail accounts.

In addition, streaming platforms such as YouTube, are not to be accessed by individuals on NYP computers, laptops, tablets and mobile phones to view films and TV programmes which are protected by copyright. Viewing such material is likely to be an infringement of copyright and place NYP at risk of substantial financial penalties. Please note this does not prevent an individual using a personal device for their sole use to view such content during breaktimes, provided they are licensed to do so under their own domestic licensing arrangements.

Information is also provided on The Source regarding the permitted use of TV, Radio and Music in the workplace. Colleagues should familiarise themselves with this.

Some things can adversely affect how our systems operate. To keep our systems safe and effective please adopt the following:

- Safeguard security controls and don't modify or alter the FORCE operating system or system configuration or attempt to circumvent or defeat security measures without express authorisation;



- Complete an asset authorisation request to obtain the prior approval from the Information Security Officer or their deputy, and if necessary the Head of Information Communication Technology (ICT), before purchasing or downloading or installing any software including any cloud-based service, even if it's free. This can affect both security and effective working of the network due to the potential introduction of malware and virus into the core architecture without the knowledge of the user. Downloads and installs are currently not permitted due to licensing and copy right issues applied to enterprise organisations
- Obtain the prior written permission of the Head of ICT and the Information Security Officer or their deputy before using encryption or other method of coding messages on the infrastructure system;
- Lock your computer screen or computer when not in use for short periods of time;
- Never share your password or log in sessions on any system, application or software.

2) Receipt of/or Accidental Access to Offensive Material or virus concerns.

If you inadvertently access a site which displays material that is inappropriate, pornographic or prohibited, immediately close the connection to the internet and report the incident to a manager. In the absence of a manager, a report should be made to the ICT Service Desk. Managers are responsible for making a record of the incident and reporting it to the ICT Service Desk. Cyber threats such as a virus, Trojan or other malware concerns must be reported to ICT Service Desk immediately, followed by the Information Security Officer via the Report and Information Security Incident form which can be found on the Intranet. If you think you may have become a victim to a cyber threat or been on an insecure or suspect site let ICT Service Desk know as soon as possible.

3) Social Networking Sites (SNS)

Please refer to the Social Media Policy.

4) Receiving and Sending Email

Please remember that email consumes a lot of energy and storage in both the cloud Microsoft 365 solutions and on premise. Limiting the size and amount of email traffic will assist with network speed and storage capacity. Good practice is encouraged, including using out of office replies, restricting size and putting network links into the body of emails rather than adding attachments. In the future mailbox limits are likely to be brought in so effective management of your email accounts, including the deletion of emails, is essential.

Emails can often be used to transport cyber threats such as malware which impact on IT networks and threaten security and integrity of data and information. If you receive an email which you believe may be from a suspicious source, please report this immediately to the ICT Service Desk. Please do not open the email or any attachments associated with it until advised to do so. For



education and awareness please read the Phishing and SPAM brief available on the Information Security page.

The auto-forwarding of emails to other email accounts is strictly prohibited and should only be done so with formal agreement of the Senior Information Risk Owner (SIRO – Deputy Chief Constable).

5) Public Service Network in Policing (PSNP) Email

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

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. CJSM continues to be a secure method of email communication.

FORCE users will be using Microsoft Office 365 and the exchange online service from early 2020. Users email domain will have changed 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 a FORCE 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, and 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 the content.

If you communicate with a local authority or governmental partners (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 Government Digital Services (GDS) new standard. You can inform 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 user(s) 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 immediately as per the Security Incident Reporting Procedure. You must delete any emails received in error and must not disseminate or use 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.

6) Recording images or audio recording on personally owned devices on FORCE premises

There have been a few occasions in the past where staff have inadvertently recorded private information when recording images or audio on their personal devices whilst at work. Please take care if using your own device, not to record official information which may be displayed on the walls or computer screens and please consider your responsibilities under Article 8 (ECHR) Right to respect for private and family life. All are reminded that personal devices such as none FORCE authorised storage mediums, cameras and other electronic devices, must not be plugged into a FORCE computer or other hardware.

7) Retention of Evidence

When using email in relation to criminal investigations, the Criminal Procedure and Investigations ACT (CPIA) 1996 must be considered. Relevant material retained should be listed on the Manual of Guidance (MG) file. Any email containing evidence may be retrieved by ICT for disclosure purposes.

8) Breach of Legislation or Policy/Procedure

Any suspected breach of legislation or this procedure must be reported to line managers, who will conduct/arrange appropriate enquiries.