Internet and E-mail Usage Procedures 2021

Procedure Owner	
Owner:	Head of Information Technology
Author:	Information Technology Security Officer (ITSO)
Screening and Proofing	
Section 75 screened:	*8th July 2021 – no further action required*
Human Rights proofed:	*8th July 2021 – no further action required*
Privacy Impact Proofed:	22nd September 2021
Consultation	
NAPO & NIPSA	23rd July 2021 – 3rd September 2021
Approval	
SLT:	5th October 2021
PPC:	29th October 2021
Board:	19th November 2021
Version	
Version:	2.0
Publication date:	
Implementation date:	
Review date:	19th November 2025

Document Control

Version No.	Date	Description
2.0	May 2021	Update after migration to IT Assist
	23rd June 2021 – 3rd September 2021	Union consultation
	14th March 2023	Minor update to contact details.

Alternative Formats

This documentation can be made available in alternative formats such as large print, Braille, disk, audio tape or in an ethnic-minority language upon request. Requests for alternative formats can be made to the Probation Board using the following contact information:

Equality Manager
Probation Board for Northern Ireland
2nd Floor
80-90 North Street
Belfast
BT1 1LD
Telephone number: 028 9052 2522
E-mail: info@probation-ni.gov.uk

Contents

1. Aim

1.1. The aim of this document is to define the Probation Board for Northern Ireland's (PBNI) procedures on internet and e-mail usage. The procedures apply to all electronic devices capable of using the internet and email. The procedures apply to all PBNI staff and Board members, as well as any third-parties making use of PBNI internet and email facilities.

2. Internet Usage Policy Provisions

2.1. IT Assist has software and systems in place that monitor and record all Internet usage on PCs, laptops, mobile phones and tablets. These systems are capable of recording (for each and every user) each internet site visit, e-mail message and file transfer into and out of the internal networks.

2.2. Users have no right to privacy when using the provided Internet and e-mail facilities. PBNI reserves the right to (i) monitor and record internet and e-mail usage at any time and (ii) inspect any, and all, files stored in any areas of its systems in order to assure compliance with its policies and any statutory or legislative obligations. Internet and e-mail activity will be reviewed periodically and usage patterns analysed. Overall activities and patterns of PBNI usage may be published.

2.3. Unless expressly identified and recorded for a business need - e.g. in connection with policy on sexual offences or the investigation of an incident - the display of any kind of sexual image or document on any PBNI system is a violation of PBNI policy on sexual harassment. This type of material may not be accessed, archived, stored, distributed, edited or recorded using the network or computing resources and could lead to complaints or breaches of the Code of Conduct.

2.4. PBNI systems must not be used to violate laws and regulations applicable in the United Kingdom. Any software or files downloaded via the Internet into PBNI systems become the property of PBNI. Any such files or software may only be used in ways that are consistent with their licences or copyrights. PBNI retains the copyright to any material posted on the Internet by any employee in the course of his or her duties.

2.5. Staff must refrain from political advocacy and from the unauthorised endorsement or appearance of endorsement of any commercial product or service.

2.6. Online social networking can be a useful business tool and, although the potential benefits are great, use of these technologies inherently carries greater risks than traditional web browsing. These risks largely come from the fact that the content of online social networks is predominantly user-generated. Damaging and/or inappropriate content can also be published and disseminated easily. These risks threaten the confidentiality, integrity and availability of the data on PBNI systems. However, the risks are not solely related to information assurance. Online social networking usage could potentially also undermine personnel safety, organisational reputation and the safety of the public who interact with an entity via these services and could lead to complaints or breaches of the Code of Conduct.

2.7. Firewalls are used to assure the safety and security of internal networks. Staff must not attempt to disable, defeat or circumvent any IT security facility.

3. Responsibilities

3.1. Staff may:

3.1.1. Use internet and e-mail facilities for reasonable personal use;

3.1.2 Make occasional use of the Internet for on-line banking or the purchase of goods and services, provided payment is made by the individual, delivery of items purchased is to a private address, and the order is not linked with your PBNI email address.

3.1.3 PBNI or IT Assist do not accept (i) any responsibility for the security of credit card details, or any other payment method used, or (ii) any liability for losses or other liabilities arising out of transactions, whether as a result of fraud or howsoever caused, suffered while using PBNI systems for personal transactions. All such use is entirely at the individual's own risk.

3.2 Staff must:

3.2.2 Respect copyrights, software licensing rules and property rights, download only software with direct business use.

3.2.3 Keep all user IDs and passwords secure as staff are responsible for all activities recorded under them.

3.2.4 Be alert to the risk of leaving an unattended machine logged on, which could lead to unauthorised use of your account. Impersonation or unauthorised use of another user's identification will be considered a breach of security. Computers must be locked (Ctrl-Alt-Del -> Lock or "Windows Key"+L) when unattended.

3.2.5 Give due regard to maintaining the clarity, consistency and integrity of PBNI's corporate image and avoid making any inferences that may prove inappropriate from a PBNI perspective.

3.3 Staff must not:

3.3.2 Use internet or e-mail facilities for unlawful purposes.

3.3.3 Disclose protectively marked information, personal data or service user data to any unauthorised party.

3.3.4 Knowingly connect to any internet site that contains inappropriate material. If staff accidentally connect to such a site, they must disconnect from that site immediately. Staff must report any such events to the PBNI Information Technology Security Officer (ITSO) immediately.

3.3.5 Use internet or e-mail facilities to carry out activities for personal gain;

3.3.6 Use internet facilities, Removable media or e-mail to download software such as music, screensavers, games, or to play games over the Internet.

3.3.7 Download videos unless there is an express work related use for the material, noted and approved by line management.

3.3.8 Use internet facilities to download any virus or program designed to infiltrate a system to gather information or other type of malicious program code.

3.3.9 Use internet facilities to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

3.3.10 Use internet facilities to connect to, or use, social networking sites (a website, which allows individuals to construct a public or semi-public online profile and to connect with others who share similar interests and views) such as Facebook, Twitter, Instagram etc. unless authorised by PBNI for work purposes.

3.3.11 Use PBNI systems to run a private business e.g. freelance or consultancy work.

3.3.12 If staff misuse the internet in any of the ways described above, they may be subject to disciplinary action. In certain circumstances this may be regarded as gross misconduct and could result in dismissal.

4 Email Code of Conduct

4.1 Users should apply similar standards to the use of e-mail as other carriers of information such as the telephone, textPhone and post. However, some special precautions are needed. E-mail is often spontaneous and can be written and issued without spending much time thinking about the content and, once sent, cannot be withdrawn.

4.2 E-mail also allows large amounts of information to be distributed very quickly and irretrievably. Therefore care and consideration needs to be given to the content of e-mail messages. In particular staff should guard against:

4.2.2 writing messages that could be interpreted as disparaging, offensive, inflammatory, libellous or harassing;

4.2.3 passing on such messages to other staff; and

4.2.4 passing on protectively marked information to unauthorised staff which is contained within the content of long e-mail chains.

4.3 As in the case of external or internal mail sent to the wrong person, it is the staff member's responsibility to ensure that e-mail received in error is properly re-directed or returned to the originator. In addition, if a staff member is the accidental recipient of Protectively Marked material or personal data, they must report the incident to the Data Protection Officer at dataincident@probation-ni.gov.uk.

4.4 If staff receive what they consider to be an inappropriate e-mail, they should forward a brief note to the sender explaining that they do not wish to receive any further e-mails of that nature. If the sending of inappropriate e-mails continues, staff should advise their line manager.

4.5 If staff receive an inappropriate e-mail from outside PBNI, ensure you can verify the sender's name and email address and treat all attachments and links with caution. If you have any concerns regarding the email please forward to spam@finance-ni.gov.uk.

4.6 Staff may make occasional use of e-mail accounts to send brief personal e-mails subject to the conditions for using e-mail set out in this policy. Personal e-mails must be clearly marked 'personal'. It is an explicit condition of using this facility that staff accept that the content of such e-mails may be accessed by IT support staff, without notice or any requirement for further consent. Staff must not use PBNI official templates and the following disclaimer should be added to the foot of the message:

"This e-mail is a personal communication and is not authorised by or sent on behalf of PBNI".

4.7 While it is not intended to undertake routine monitoring of the content of e-mails (personal or otherwise), e-mail traffic may be accessed at any time either as a result of checking an officer's e-mail account for business reasons if they are absent from work, or as part of an exercise to monitor compliance with the Internet and E-mail Usage policy;

4.8 Staff must not use the e-mail system to send or store sexual or offensive material. If staff receive any such inappropriate material via e-mail they must report the incident to the ITAssist Service Desk on 155 (0300 1234 155) or itassist@nigov.net immediately;

4.9 Staff must not promote or participate in "chain mail". Chain mail is when you are asked to send a particular message to a number of other people who are also asked to send it on. These messages commonly promise good luck, success or help for charitable causes. They are designed to be annoying and/or damaging, and they slow down computer systems. Staff should delete any such mail immediately upon receipt;

4.10 If staff have completed work at home on home equipment, which has been authorised and is not protectively marked, it may be forwarded to their PBNI e-mail address.

4.11 Staff must use the Automatic Replies (Out of Office) function within Microsoft Outlook to inform customers and colleagues if you are unavailable. If away unexpectedly, BSMs may raise a Service Request with IT Assist to activate the Automatic Replies (Out of Office) function Assistant with an appropriate message.

5 Email security

5.1 OFFICIAL SENSITIVE information must not be sent to personal email addresses.

5.2 All gov.uk and cjsm email addresses are secure and OFFICIAL SENSITIVE information can be emailed to these addresses without additional protection. All email traffic between @probation-ni.gov.uk and @psni.police.uk is encrypted, and again information can be emailed between these addresses without additional protection.

5.3 If OFFICIAL SENSITIVE information is to be sent to other organisations it must be encrypted using 7-zip and sent as an attachment. 7-zip can be installed via the "IT Assist Store" icon on your desktop.

5.4 If staff are transmitting OFFICIAL SENSITIVE information, they must ensure, as far as possible, the e-mail contains the words “OFFICIAL SENSITIVE” at the top of the covering e-mail and all attachments are similarly marked.

6 Storing emails

6.1 To enable compliance with a wide range of statutory duties and responsibilities, PBNI has a duty to keep a permanent record of all significant documents.

6.2 An email (including attachments) should be saved if it:

6.2.2 provides the only evidence of the origin of and/or date of receipt of an attached document which needs to be retained;

6.2.3 records decisions or provides authority for action;

6.2.4 will be needed to maintain business continuity;

6.2.5 might be needed for administrative, accounting, audit, research or historical purposes;

6.2.6 might be needed to prove whether an activity or transaction took place; and/or

6.2.7 could be requested under the Data Protection or Freedom of Information provisions.

6.3 Any information relating to service users must be stored in ECMS.

7 Internet and Email monitoring

7.1 Monitoring of internet usage and emails of employees in PBNI is carried out within legislative requirements.

7.2 It is PBNI’s duty to ensure that:

7.2.2 Staff can work in a safe and harmonious work environment;

7.2.3 Staff do not breach national security guidelines;

7.2.4 Staff do not engage in criminal activity;

7.2.5 Staff do not engage in activities likely to bring the reputation of PBNI into question;

7.2.6 Staff do not otherwise abuse their conditions of employment.

7.3 Monitoring of internet and e-mail is carried out to:

7.3.2 block the sending or receiving of inappropriate e-mails;

7.3.3 monitor all outbound e-mail for any potential security leak so that evidence can be investigated;

7.3.4 examine logs of websites visited to check that staff are not downloading inappropriate material or information of a criminal nature or that will seriously affect the reputation of PBNI.

8 Non Compliance

8.1 Failure to manage information in accordance with these procedures may result in disciplinary and/or criminal action. Any breach, or suspected breach, of these procedures must be reported to Line Management and the PBNI ITSO. Any potential breach will be subject to investigation which may result in disciplinary action. In certain circumstances a breach of this policy may be regarded as gross misconduct and may lead to dismissal.

8.2 The following are some examples of what will be regarded as a breach of these procedures and subject to disciplinary investigation. The list is not exhaustive but is representative of areas or issues that staff should be especially vigilant about:

8.2.2 deliberate access of inappropriate or offensive material;

8.2.3 attempting to use the internet to obtain software for personal use e.g. screen savers or games;

8.2.4 sending messages which are abusive, offensive, libellous or could be perceived to be harassment or bullying;

8.2.5 generating and/or distributing chain e-mail;

8.2.6 using Internet or e-mail facilities for political or commercial activity;

8.2.7 disseminating or printing copyright material in violation of copyright laws.

8.3 Staff should be aware that the possession of child abuse images is a serious criminal offence. PBNI will fully co-operate with law enforcement authorities to identify and take action against any member of staff accessing, possessing or disseminating such material. Individuals found to have been involved in any way in the possession or dissemination of child abuse images may face serious disciplinary action with a high probability of dismissal irrespective of whether or not they are prosecuted or convicted under the criminal law.

8.4 Unless expressly identified and recorded for a business need, the use of PBNI systems to disseminate inappropriate material which could cause offence to others (irrespective of whether any offence is intended) may constitute harassment and will not be tolerated and may constitute gross misconduct. Inappropriate material may include, but is not limited to, any material of a pornographic, homophobic, sexist, racist, sectarian, violent or offensive nature or that uses disablist language, whether in pictures, cartoons, words, sounds, or moving images, and whether or not purporting to be of a humorous nature.

9 Contacts, Enquiries and Advice

9.1 If you require any further information on these procedures, you should contact:

TITLE	EMAIL / PHONE
PBNI IT Security Officer	Colin.Barnes@probation-nl.gov.uk 07785696225
DoJ IT Security Officer	doj.itso@justice-ni.gov.uk
PBNI Data Protection Officer	Kyle.Tweedie@Probation-NI.gov.uk 07887510159