Internet and E-Mail Usage Policy 2021

Policy 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	
NIPSA & NAPO:	*23rd July 2021 - 3rd September 2021*
Approval	
SLT:	*05th October 2021*
Board:	*19th November 2021*
Version	
Version:	V2.0
Publication date:	
Implementation date:	
Review date:	*19th November 2025*

Document uncontrolled when printed

Document Control

Version No.	Date	Description
1.1	October-November 2015	Union Consultation
1.2	3 November 2015	Draft for approval by SMT
1.3	11 December 2015	Draft for approval by Board
1.4	11 December 2015	Approved by Board
2.0	June 2021	Version 1 reviewed and updated to draft Version 2.
	23rd July 2021 – 3rd September 2021	Union Consultation
	5th October 2021	Draft for approval by SLT
	29th October 21	Draft for approval by PPC.
	19th November 2021	Approved by Board.
	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

Section		Page
1.	Rationale	
2.	Aim	
3.	Objectives	
4.	Procedures	
5.	Resources	
6.	Communication and Training	
7.	Monitoring	
8.	Review	
9.	Non-compliance	
10.	References	
11.	Contacts, Enquiries and advice	

1. Rationale

This policy sets out the principles and working practices that are adopted by PBNI for access to the internet and e-mail so that the risk of loss, or corruption to business data are mitigated. The policy and processes are applicable to all information, including paper records, computers, communications systems and the information stored and processed on them as well as other information assets in PBNI.

The policy applies to all fixed and mobile device equipment provided to staff. This includes, but is not restricted to, PBNI supplied and supported personal computers, laptops, mobile phones, smartphones, tablets and approved external storage devices which can be used to access, store, process, transmit, discuss, or record data electronically.

PBNI provides access to the internet and e-mail. PBNI expects its staff (as defined below) to use these resources for work related purposes during core hours i.e. to communicate with colleagues and relevant third-parties, to research relevant topics and to obtain useful work related information.

PBNI insists that staff must, at all times, conduct themselves honestly and appropriately and respect the copyrights, software licensing rules, property rights, and privacy of others. All existing PBNI policies about personal conduct apply equally when using e-mail or the internet.

Particularly relevant are those that deal with misuse of resources, copyright, offensive material, harassment and bullying, confidentiality and data protection, and information assurance.

Unlawful internet usage may lead to negative publicity for PBNI and may expose it to significant legal liabilities. Unlawful internet usage may lead to disciplinary action and civil or criminal proceedings.

Anything that an employee writes in the course of acting for PBNI on the internet or in an e-mail could be taken as representing PBNI's official line. That is why PBNI expects staff to take particular care when participating in electronic communications using PBNI resources.

Whilst the internet offers a wealth of potential benefits, it can open the door to some significant risks to PBNI systems if appropriate security procedures are not followed. The government's more general and underpinning Security Policy Framework (SPF) www.gov.uk/government/publications/security-policy-framework continues to apply.

As with the Social Media Policy paper, we should include at this point who the policy applies to:

For the purposed of this policy, “staff” includes PBNI Board members, full-time staff, part-time staff, agency staff, placements and volunteers. This policy also applies to any Third Parties making use of PBNI Internet and E-mail facilities.

2. Aim

The aim of this document is to define PBNI’s policy and to help staff understand the expectations for the use of internet and e-mail facilities. This policy also should be read in conjunction with the following documents:-

- HMG Security Policy Framework (SPF)
- PBNI Risk Management Policy
- PBNI Data Protection Policy and Guidance
- PBNI Freedom of Information Policy
- PBNI Records Management Guidance
- PBNI Social Media Policy
- PBNI Internet & E-mail Usage Procedures
- PBNI Mobile Device Security Policy and Procedures
- PBNI Disciplinary Policy
- PBNI Code of Conduct for Staff

3. Objectives

- To make the effective management of internet and e-mail usage an integral part of overall management practice.

- To raise awareness of the need for monitoring internet and e-mail usage by all within PBNI.

- To have a policy in place to support the statement on internal control, and corporate governance arrangements.

4. Procedures

There are accompanying Internet and E-mail Usage Procedures which support the application of this policy.

5. Resources

This policy will not incur any additional cost.

6. Communication and Training

This policy will be communicated to all staff, and will accessible via the intranet.

7. Monitoring

This policy will be kept under review to ensure it is in keeping with current legislation and good practice.

All staff are responsible for the success of this policy and should ensure that they read and understand it.

8. Review

This policy will be reviewed within four years from date of approval. Interim reviews may also be prompted by feedback and/or identified changes in law or practice.

9. Non Compliance

Failure to manage information in accordance with relevant PBNI policies, procedures or guidance and appropriate legislation may result in disciplinary and/or criminal action.

10. References

Data Protection Act 2018
The Freedom of Information Act 2000
The Information Commissioner's Office
HM Government – Cabinet Office guidance
The National Archives
The Public Records Office Northern Ireland (PRONI)
United Kingdom General Data Protection Regulation (UKGDPR)[1]
Directive (EU) 2016/680: The Law Enforcement Directive (LED)

11. CONTACTS, ENQUIRIES AND ADVICE

If you require any further information on this policy, in the first instance 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

[1] The DPPEC (Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit)) Regulations 2019 previously EU Regulation 2016/679: The General Data Protection Regulations (GDPR)