

Internet and E-mail Usage Policy

Policy Owner	
Owner:	Head of Information Technology
Author:	Information Technology Staff Officer
Screening and Proofing	
Section 75 screened:	<i>18 November 2015</i>
Human Rights proofed:	<i>17 November 2015</i>
Consultation	
	<i>Union consultation – October-November 2015</i>
Approval	
SMT:	<i>3 November 2015</i>
Board:	<i>11 December 2015</i>
Version	
Version:	1.0
Publication date:	
Implementation date:	<i>11 December 2015</i>
Review date:	<i>No later than December 2019</i>

Contents

Section		Page
1	Rationale	4
2	Aim	4
3	Objectives	5
4	Procedures	5
5	Review	5
6	Non Compliance	5
7	Contacts, Enquiries and Advice	5

1. Rationale

This policy supports compliance with the Information Assurance Policy in respect of internet and e-mail usage.

This policy sets out the principles and working practices that will be adopted by PBNI for access to the internet and e-mail so that the risk of loss, or corruption to business data is low. 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 electronic devices provided by PBNI. The policy applies to all PBNI staff and Board members.

PBNI provides access to the internet and e-mail. PBNI expects staff to use these resources for work related purposes during core hours i.e. to communicate with colleagues, 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 security. Unlawful internet usage may lead to negative publicity for PBNI and may expose it to significant legal liabilities. Unlawful internet usage may lead to 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. These procedures are outlined in the PBNI Information Security Procedures and the HMG Security Policy Framework (SPF).

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 Information Assurance Policy
- PBNI Information Security Procedures
- PBNI Monitoring at Work Procedures
- PBNI Risk Management Policy
- PBNI Disciplinary Policy
- PBNI Internet & E-mail Usage Procedures

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. Review

This policy will be reviewed within four years from date of approval.

6. 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.

7. Contacts, Enquiries and Advice

If you require any further information on this policy, you should contact:

TITLE	EMAIL / PHONE
IT Security Officer	infosec@pbni.gsi.gov.uk 02890 262516
IT Helpdesk	helpdesk@pbni.gsi.gov.uk 02890 262432