

PRESCRIPTION PRICING AUTHORITY COMMUNICATIONS AND PRIVACY POLICY

1 INTRODUCTION

At the Prescription Pricing Authority (PPA), communication plays an essential role in the conduct of our business. The PPA values your ability to communicate with colleagues and business contacts.

The PPA trusts you to use the information technology and communications facilities sensibly, professionally, lawfully, consistently with your duties, with respect for your colleagues and in accordance with this policy and with the PPA's rules and procedures.

2 THE NEED FOR A POLICY

How you communicate with people not only reflects on you as an individual but on the PPA as an organisation. Although the PPA will respect your personal autonomy and privacy, it has established this policy to let you know what is expected from you and what you can expect from the PPA in your use of e-mail, the Internet and other means of communication such as paper correspondence, fax, fixed line or mobile phones (including SMS text messages).

There are various laws and acts of parliament that have influenced and/or required the production of this policy. These are as follows:- (please note this is not an all encompassing list)

- The Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Obscene Publications Act 1959
- Telecommunications Act 1984
- The Children Act 1978
- Criminal Justice Act 1988
- Copyright, Design and Patents Act 1998
- Protection from Harassment Act 1997
- Sex Discrimination Act 1975
- Race Relations Act 1976
- Computer Misuse Act 1990

3 GENERAL PRINCIPLES

Note that in this policy, "*traffic data*" means the data used to facilitate communications (e.g. between computers) **but not** the content of that communication.

In general:

- All paper-based and electronic information is expected to be treated in a confidential manner.
- As an employee, you should exercise due care when collecting, processing or disclosing any personal data and process personal data on behalf of the PPA only when it is necessary for you to do your job.
- All equipment provided to you by the PPA to carry out your business function must be used for authorised business purposes only.
- This policy does not cover the management of the quality of communications. You should make reference to individual directorate's quality control policies/procedures for the authorised release of communications.
- As the PPA is a responsible employer, this policy has been issued to you to ensure that you are aware of what communications will be monitored and how that monitoring will take place.
- As part of normal business activity it is expected that line management will require access to correspondence produced or received by you. This access may or may not occur in your presence as required by the business.

4 USE OF ANY COMMUNICATION MEDIUM

The advantage of the Internet and e-mail (both internal and external) is that it is an extremely easy and informal way of accessing and disseminating information. However, the same principles apply to information exchanged in this way as apply under the terms of your employment contract to any other means of communication. For example, sending defamatory, sexist or racist jokes or other material can constitute grounds for an action for defamation, harassment or incitement to racial hatred in the same way as making defamatory, sexist or racist comments to a colleague. Therefore, do not use the Internet, e-mail or SMS text (both internal and external) for purposes that would be subject to disciplinary or legal action in any other context. If you are in doubt about a course of action, take advice from your line manager.

The PPA expects its staff, at all times, to communicate in a professional manner whether the communication is internal or external.

The PPA expects its staff to use the provided communication mediums for the authorised use they were intended.

Care must be taken when using e-mail (internal or external), fax, mobile phone SMS text messages or letter as a means of communication because all expressions of fact, intention and opinion may bind you and/or the PPA and can be produced in court in the same way as oral or written statements.

5 USE OF INTERNET, INTRANET AND NETWORK SERVICES

The PPA provides you with access to the internet for the discharge of your business duties (as authorised by your line manager) and for personal use, in non-work time. In terms of both business and personal use, the PPA expects you to act in a professional and lawful manner, consistent with your duties and with respect for your colleagues

The PPA allows all employees access to the internet for personal use either from individual desktop PCs or from designated Internet access PCs.

You should understand the worldwide nature of the Internet. Internet communication or any information received may pass through any number of intermediate computers and countries. Therefore personal or financial information sent via the Internet must be considered insecure. Communications are at risk of being read en route. Careful consideration should therefore be given to the content of any communication.

The PPA is not responsible for the content of websites other than our own. Whilst we have made every effort to block access to those sites that contain potentially offensive material, it is possible that you may still be able to access such sites. Please advise the PPA Information Security Manager accordingly.

When you access the Internet a challenge will be made asking for you to confirm your acceptance of this policy before access will be allowed. The text of this challenge is detailed in Appendix A

5.1 Acceptable Use

Business use of the internet is permitted as authorised by your line manager.

Personal use of the PPA's Internet facility is permitted within your own time, provided that this does not interfere with performance of the system. These services will be available during the normal business hours of the office or building in which you work. Within this time, the PPA Internet facility may be used outside of your scheduled hours of work, provided that such use is consistent with professional conduct and in accordance with this policy. No level of service availability or performance is guaranteed, business needs will take priority.

5.2 Unacceptable Use

5.2.1 General

You **must not**, in the absence of formal authority from a senior IT manager responsible for the operation of the IT or communications system:

- introduce packet-sniffing or password detecting software which can monitor the use of computers, systems or data by others;
- access any device or tool that you have not been authorised to use;
- knowingly seek unauthorised access to data which you know, or ought to know, is confidential; nor
- attach any device or tool to the PPA's network that you have not been authorised to use.

The PPA's Internet connection **MUST NOT** be used for any purposes such as those which:

- Violate any PPA policies
- To transmit over or place on the Internet any sensitive / confidential PPA information without the written permission of a director.
- For the operation of a personal business through the PPA internet link.

5.2.2 Abuse

The following general actions are strictly prohibited:

- Any conduct which violates the PPA Standards of Business Conduct. PPA reserves the right, in its sole discretion, to make a determination whether any particular conduct violates such norms and expectations.
- Any conduct that restricts or inhibits any other employee, whether another employee of the PPA or an employee of any other system or network, from using any of PPA's services or products, as determined by PPA at its sole discretion.
- Harassment, whether through language, frequency, or size of messages.
- Creating, forwarding, posting, or distribution of chain messages of any type.
- Forging of message headers or a sender's identity, or taking any similar action with the intent of bypassing restrictions or limits on access to a specific service or site (such as a

moderated newsgroup or a site utilising filters). This prohibition does not restrict the legitimate use of aliases.

- Falsifying identity or contact information to circumvent this Policy.
- Attempting to circumvent or alter the processes or procedures to measure time, bandwidth utilisation, or other methods to document traffic data.

5.2.3 Illegal Use

PPA IT equipment / systems may be used only for lawful purposes. The transmission, distribution, or storage of any information, data, or material in breach of any applicable law or regulation is prohibited. Without limitation of the foregoing, it is strictly prohibited to create, transmit, distribute, or store any information, data, or material which:

- Infringes any copyright, trademark, trade secret, or other intellectual property right.
- Is obscene or constitutes child pornography.
- Is libellous, defamatory, hateful, or constitutes an illegal threat or abuse.
- Violates export control laws or regulations.
- Encourages conduct that would constitute a criminal offence or give rise to civil liability.

5.2.4 Security

Breaches of system or network security are prohibited, and may result in criminal and / or civil liability. PPA will investigate potential security breaches, and may notify the appropriate law enforcement authorities where applicable.

It is strictly prohibited to attempt to circumvent the authentication procedures or security of any host, network, network component, or account (e.g. "cracking") to access data, accounts, or servers which the employee is not expressly permitted or authorised to access. This prohibition applies whether or not the attempted intrusion is successful, and includes unauthorised probes or scans performed with the intent to gather information on possible security weaknesses or exploitable configurations.

You are prohibited from interfering or attempting to interfere with service to any other user, host, or network on the Internet (e.g. "denial of service attacks"). Examples of such prohibited activity include without limitation:

- (a) Sending massive quantities of data with the intent of filling circuits, overloading systems, and / or crashing hosts
- (b) Attempting to attack or disable any user, host, or site

- (c) Using, distributing, or propagating any type of program, script, or command designed to interfere with the use, functionality, or connectivity of any Internet user, host, system, or site.

You are prohibited from intentionally or negligently propagating computer worms, viruses or other potentially malicious code.

5.2.5 E-Mail

You are prohibited from engaging in improper use or distribution of electronic mail ("e-mail") over the Internet. Without limitation of the foregoing, it is strictly prohibited to engage in any of the following activities:

- Sending unsolicited bulk e-mail ("UBE", or "spamming").
- Setting up "mail back" or "drop box" addresses in order to receive responses from UBE, either directly by the employee or by a third party on behalf of the employee.
- Send or encourage "letter bombs." Letter bombs are extremely large or numerous e-mail messages that are intended to annoy, interfere, or deny e-mail use by one or more recipients.
- Sending sexually explicit messages or images whilst using PPA IT systems / equipment
- Sending personal e-mails to the business e-mail accounts of colleagues

5.2.6 World Wide Web

PPA strictly prohibits you from engaging in any of the following web-related activities:

- Excessive use of bandwidth by utilising programs, scripts, or commands to abuse a web site (for example, by connecting for an excessive amount of time, repeatedly engaging site-local scripts, or related behaviour).
- "Walking" a database for the purpose of collecting data contained therein (whether or not this behaviour requires that the reader of the page must knowingly ignore files such as "robot.txt" which is designed to guide cataloguing robots/programs).
- Operating a robot on a site's page after the site has asked that the behaviour cease.
- Intentionally or negligently viewing material of a dubious nature. If you unintentionally find yourself connected to a site which contains such material you must disconnect from the site immediately and inform the PPA Information Security Manager.

The PPA will make best efforts to automatically block access to sites that contain offensive material (i.e. pornography, etc.).

6 PERSONAL RESPONSIBILITIES

For your information, this paragraph lists three activities which are criminal offences under the Computer Misuse Act 1990, and a fourth offence which is an offence under the Data Protection Act 1998:

- gaining unauthorised access to computer material (e.g. hacking, using someone else's password);
- making unauthorised modifications to the contents of a computer (e.g. to data or software);
- gaining unauthorised access to a computer with intent to commit/facilitate the commission of further offences; and
- unauthorised obtaining or disclosing of personal data (or information contained in the data) without the authority of the PPA.

Downloading, copying, possessing and distributing material from the Internet may be an infringement of copyright or other intellectual property rights. The same applies to paper-based documents. If you are uncertain as to whether you can make copies of an item, contact your line manager for advice.

Familiarise yourself with relevant responsibilities associated with the PPA's security policies and procedures (e.g. those associated with structure of passwords, remote working). The following serve as a reminder of two important areas:

- Do not use the system in any way, which may damage, overload or affect the performance or the internal or external network.
- Use information only for the purposes for which it was supplied or obtained and do not disclose to any unauthorised third party. This duty of confidence applies even if you have left the employment of the PPA.

6.1 Data Protection Act 1998

In relation to personal data, whether you are working at the PPA's premises or working remotely, you must:

- keep them secret and confidential and you must not disclose them to any other person unless authorised to do so by the PPA. If in doubt ask your line manager or the Information Security & Data Protection Manager for advice;

- familiarise yourself with the provisions of the Data Protection Act 1998 and comply with its provisions;
- process personal data strictly in accordance with the Data Protection Act 1998, the PPA's data protection policy and other policies and procedures issued by the PPA; and
- avoid making personal or other inappropriate remarks about clients or colleagues on manual files or computer records. This does not mean that you cannot record information or opinions, which the individual concerned views as detrimental, but they must be justifiable.

The PPA views any deliberate breach of the Data Protection Act 1998 and our data protection policy as gross misconduct which may lead to summary dismissal under our disciplinary procedures.

If you make, or encourage another person to make, an unauthorised disclosure of personal information knowingly or recklessly then you may be held criminally liable.

When you are working remotely, you must:

- protect any work which relates to the PPA's business so that no other person can access your work;
- position yourself so that your work cannot be overlooked by anyone else;
- take reasonable precautions to safeguard the security of all equipment provided to you by the PPA to carry out your business function;
- take reasonable precautions to protect the integrity of password(s) you use;
- apply an appropriate level of security to any information or personal data which comes into your knowledge, possession or control through your employment with the PPA so that the personal data are protected from theft, loss, destruction or damage and unauthorised access and use;
- inform the police and/or our IT Department as soon as possible if any equipment provided to you by the PPA has been stolen;
- inform the IT Department if you think the security of the data on your laptop has been compromised - do not worry if your suspicions are unfounded; it is better to be safe than sorry; and

- ensure that any work, which you do remotely, is saved on the PPA's system or transferred to the PPA system as soon as reasonably practicable.

7 MONITORING COMMUNICATIONS

The PPA will respect your privacy and autonomy in your communications. However, in certain circumstances it may sometimes be necessary to access and record your outgoing and incoming communications for purposes, which include the following:

- providing evidence of business transactions;
- responding to a customer complaint;
- making sure the PPA's business procedures are adhered to;
- training and monitoring standards of service;
- preventing or detecting unauthorised use of the PPA's communications systems or criminal activities;
- maintaining the effective operation of the PPA's communication systems.

The PPA routinely monitors telephone (fixed line and mobile), fax, e-mail and Internet traffic data for payment, audit and capacity planning purposes.

8 FAILURE TO COMPLY

Failure to comply with this policy may lead to disciplinary action being taken against you under the PPA's disciplinary procedures, which may lead to summary dismissal.

Breaches in any appropriate laws may lead you to the commission of criminal offences which would be dealt with in the appropriate manner.

It is therefore important that you read this policy carefully. If there is anything in it that you do not understand, please discuss it with your line manager, who may seek clarification from the PPA Information Security Manager.

Non-adherence to this policy may expose you to civil action through the courts.

9 VALIDITY OF THIS POLICY

This Policy is designed to avoid discrimination and be in accordance with the Human Rights Act 1998 and its underlying principles.

This policy will be reviewed annually under the authority of the Chief Executive.

D.G.Ball
Data Protection Officer
30th March 2003

APPENDIX A – Electronic message Confirmation of Acceptance / Understanding

When you connect to the internet the words shown below will be displayed on the personal computer with an acceptance button to be clicked and hence provides confirmation of your understanding and acceptance of this policy. You are not allowed to access the internet unless you accept the statement below:-

“By clicking on the OK button I am confirming that I have seen and read a copy of the PPA Communications and Privacy Policy (*a hyperlink to the policy will be included here*). I understand the terms of the Policy and agree to abide by it. I understand that security software may record the use I make of the Internet, which may include logging the addresses of any web sites and noting what file transfers I make. I have no objection to any monitoring of the use I make of any NHS establishment IT equipment. I understand that any violation of this policy could result in disciplinary action, and possibly dismissal or criminal prosecution.”