PROTOCOL – INFORMATION TECHNOLOGY FOR MEMBERS

1. Introduction

This document sets out the terms and conditions under which information technology facilities are to be made available to assist Members to carry out

their duties. The Conditions are also intended to ensure that Members comply with relevant computer related legislation. A brief summary of relevant Acts is attached as Annex 1.

2. Definition

For the purposes of this document the term 'system' refers to:

i. the hardware provided

ii. the software provided

iii. the telecommunications equipment and lines provided

iv. data stored on or processed by the hardware and software

v. any other Authority/Force computer system or data accessed by items i to iv

The system may be fixed (ie, desktop PC, peripherals and broadband internet connection) or portable (ie, blackberry).

3. Ownership

The system provided remains the property of the West Yorkshire Police Authority and must be returned to the Authority

- upon the Member's appointment ceasing
- if the scheme is terminated
- in the event of misuse or breach of this Protocol
- at the request of the Executive Director for maintenance, upgrade or modification

4. Installation

Officers of the Police Authority or the Force's IT Department will undertake installation of fixed systems. The Authority will provide a Broadband line (except where an agreement has been made with the Member for the Police Authority to connect to an existing Broadband line provided privately or by the Member's employer) should the Member opt for a fixed system. Members will be responsible for appropriate power sockets and for compliance with Health and Safety legislation.

The Authority will pay the monthly rental for portable systems.

5. Care of the System

The system is insured by the Authority. However it is the Member's duty to take all reasonable steps to safeguard the system against accidental or deliberate damage, theft, vandalism, misuse and loss.

6. Purposes for which the System may/may not be used

a) The system is intended to be used by the Member for Police Authority business to assist in carrying out Authority duties. Although peripherals, such as monitor, keyboard, printer etc., may be connected to and used with another computer used by the Member to avoid unnecessary duplication of equipment, the processor (hard drive) must never be used in connection with a Member's commercial business interests.

b) The system may be used for private use or, provided that prior approval is obtained in writing from the Executive Director, for non-commercial activities of a public nature, e.g. where a Member is also a Member of another public body.

Where a Member uses the system for private and/or approved business use ("private use") then the Member must pay an annual contribution towards the cost of the system in accordance with Annex 2.

c) Any data accessed through the system MUST ONLY be used for the purposes of carrying out Authority business. It must NOT be used for any other purposes. To do so may constitute misuse.

7. Persons who may use the system

Only the Member to whom it is issued may use the system.

8. Software Copyright

The system is supplied with a number of software packages already installed for Members use. The Authority properly licenses all such software.

9. Data Protection Act 1998

In the event of any data relating to individual persons (personal data) being recorded on the system then the Member must ensure that the provisions of the Data Protection Act are complied with.

Any software application designed to hold or access such data and supplied by the Authority/Force will have the purpose duly registered by the Force on the Member's behalf.

10. Security

Access to the Members' area of the website is password controlled. Members should keep their password secure and maintain the integrity of the system. Confidential items should not be stored or sent electronically.

11. Monitoring

The system is not routinely monitored by the Authority or audited for content. The content of messages to the individuals involved is private. However, the Authority reserves the right to inspect the content of all messages and communications within the system.

[NOTE The inclusion of the paragraph above is there to protect the West Yorkshire Police Authority and its Members. If it came to light there was a need to make such an inspection, the WYPA would need to authorise an officer or officers to do this. The implication is that such action would need to be authorised by the Authority, after receiving a suitable report about the issues and that officers could not decide to take such action themselves.]

12. Computer Viruses

Members must be aware of the threat from computer viruses, take due care not to introduce them to the system, and use the anti-virus facilities provided.

The system will have anti-virus measures installed but no system is 100% foolproof. Viruses are discovered at a rate of approximately 500 a month, and as a result, the anti-virus software requires updating at regular intervals. This will happen automatically through the internet.

13. Back up

It is the responsibility of Members to ensure that proper back up copies of data are taken at appropriate intervals to ensure that data is not lost if the computer crashes.

14. Consumables

The Authority will pay for these items.

15. Training

Training for Members will be arranged and paid for by the Authority.

16. Freedom of Information

Under the Freedom of Information Act 2000, all documents held by the Authority and stored on Authority systems are potentially disclosable. Members should manage their document storage and, in respect of Authority documents, apply the disposal criteria set out in the Authority's Record Disposal Procedure.

ANNEX 1

Summary of relevant legislation

This annex gives a very brief summary of legislation relevant to the use of computers and software. It does not attempt to explain every detail of the legislation.

Theft Acts 1968 and 1978

Under the Theft Act 1968 it is a criminal offence dishonestly to use, keep, deal with or take possession of any other person's property with the intention of permanently depriving that other person of it.

In this context "property" includes money or any other property, including intellectual property, and would include I.T. hardware, software and any related equipment, installation or facility.

Under the 1978 Act it is also a criminal offence to obtain services or evade any liability for payment by deception, or to deliberately "make off" without paying for goods or services supplied.

Computer Misuse Act 1990

This Act makes it a criminal offence for an authorised person to attempt to access systems or information within systems, or to attempt to exceed the facilities and privileges granted to them.

Data Protection Act 1998

This Act regulates the manner in which information relating to individuals is to be collected, processed, and used. The Act lays down 8 principles, which must be followed in relation to all personal data:-

- Process it fairly and lawfully;
- Obtain it only for one or more lawful purposes;
- Only hold it if it is adequate, relevant and not excessive in relation to the purpose for which it is processed;
- Ensure it is accurate and up-to date;
- Do not keep it longer than necessary;
- Process it in accordance with the rights of the individuals to whom it relates;
- Take appropriate steps to prevent unauthorised access and accidental loss or destruction;

- Do not transfer it outside the European Economic Area unless an adequate level of protection for the rights of data subjects applies.

All Authority/Force computer systems containing any personal data about identifiable individuals must be registered with the Data Protection Registrar.

Copyright Designs and Patents Act 1988

This Act, broadly, gives protection to the owners of software to prevent unauthorised use of their products, ie without a proper licence.

An illegal user of a computer program - ie someone who is using the program without a proper licence - can, under the Act, be liable to damages, an injunction and considerable costs. He or she could also be faced with a fine of up to £2,000 or up to six months imprisonment.

ANNEX 2

Proforma for Recharge of Private Use of the Authority's IT System

Member .....

Financial Year .....

I *have/have not used the Police Authority's IT facilities for private use.

(delete as appropriate)

I understand that if I **have** used the Authority's IT facilities for private use that I will be charged a fixed contribution of £26 per annum.

Signed .....

Date .....

Office Use

Invoice sent	
Payment received	