APPENDIX 8

THURROCK COUNCIL

Remote Access (Supporting Document)

Version Control Sheet

Title:	**Remote Access (Supporting Document**
Purpose:	**The advise staff of the councils policy and procedures regarding remote access to the councils network**
Owner:	**Information Manager –Organisational Development** **lhenley@thurrock.gov.uk** **01375 652500**
Approved by:	**Cabinet**
Date:	**19th January 2005**
Version Number:	**1.1**
Status:	**Final**
Review Frequency:	**Yearly**
Next review date:	**19th January 2006**
Consultation	**This document was sent out for consultation to the following:** **Head of e-government** **Head of Organisational Development** **Head of Audit Services** **Head of Legal Services** **Principal Business Analysts** **The PIN Group (people information network)** **Unison** **Vertex**

Remote Access to Thurrock Council Computer Network
Remote access to the council network is provided by Thurrock Council to enable authorised staff, elected members and third parties to connect to Council systems from sites where a direct connection to the council's computer network is not available. This is done through two main channels, the Remote Access Service (RAS) and Virtual Private Networks (VPN). The following guidance is intended to make staff aware of the requirements when using either method to connect to the Thurrock Council computer network.

General Standards
When using either method of connection you should be aware of the following:

1. You must comply with Thurrock Council's *ICT Policy* and with all published standards and procedures for processing information and using the authority's facilities.
2. You must have signed to state you agree to comply with the *ICT Policy* and other policies applicable to Remote Access.
3. You must not leave equipment connected to the service and unattended as the lack of physical security for remote access equipment creates a higher risk of unauthorised people gaining access to our information.
4. You must notify your authorising manager as soon as you no longer need your RAS account. This reduces the risk of security breaches.
5. As the remote access service is provided for business use only, do not use it for personal activities.
6. At no time should staff with remote access provide their username, password or other identification information used to access the Thurrock computer network to anyone, even to family members.
7. Only Council supplied and approved equipment is allowed to remotely connect to the Councils network.

Remote Access Service (RAS)
The Remote Access Service is defined as dial-in access that uses, but is not limited to, dial-in modems, ISDN and GPRS etc. From a user point of view this is normally any type of connection that uses a standard phone line. The only exception is 'broadband' (ADSL, SDSL etc) which uses a modified phone line service.

To maintain information security and make efficient use of the service you must follow the following standards:

1. Staff with remote access privileges must ensure that their Personal Computer or workstation, which is remotely connected to the Thurrock Council computer network is not concurrently connected to any other network e.g. Home Broadband

2. As far as possible, create emails offline prior to logging in. This will help to minimise the overall time you are connected to the network because the email session will send unsent emails at the same time as synchronising.
3. Unless you are using other network systems, close down your email session and disconnect the RAS link as soon as your online and offline email accounts have synchronised. This makes more ports available and reduces service congestion.
4. If working off-site, log in remotely two to three times each day to minimise the time it takes for your email account to synchronise.
5. If you are expecting to spend more than twenty minutes without accessing networked systems, disconnect from the RAS service. Inactive connections unnecessarily reduce the service available to other users.

Virtual Private Networks (VPN)
Virtual Private Networks are used to access the Thurrock Council computer network where there is an existing connection to the Internet. A VPN creates a secure 'tunnel' from their equipment through to the council network to protect any data sent or received from being viewed by a third party. However because the users equipment is connected directly to the internet the following measures need to be adhered to ensure the security of information exchanged using the connection:

1. Only equipment owned and managed by Thurrock Council can be used to connect using VPN
2. You must not change the settings on the firewall or other equipment used.
3. You must ensure that the PC has up to date anti-virus definitions

If you are unclear on any of the above please contact the E-Government Helpdesk who will be able to provide advice.

Remote Access to External Networks
Staff who are approved to use a dial up facility to connect to an external network must ensure that the equipment is not connected concurrently to the external network and the councils network. If in doubt please seek the advice of the IT Helpdesk before making a connection. An external network is any network that does not form part of the councils managed network.

Remote Access to NHSnet
Staff using a remote access service will need to be strongly authenticated before they are allowed access to systems on NHSnet.

Authentication
Authentication is essential to the security of any computer system to ensure users accessing the system are who they say they are. You currently authenticate yourself whenever you log on to the council's computer network when you enter you name and password.

However for connections from external networks it is necessary to have more secure methods of authenticating users. One way of doing this is through the use of tokens. Token-based authentication works on the 'something you have' and the 'something you know' principle.

The something you have can either be a smart card, fingerprint, time synchronized pin code etc and the something you know is usually a password. In this way we can check your identity twice (by using both the token and the password) before allowing you to access the system. This is known as two factor strong authentication.

Monitoring

Thurrock Council will undertake automated collection of service information to monitor whether the service is efficient, effective and meets business needs. Monitoring of individuals will not be undertaken unless it is necessary to prevent or detect crime or to ensure that the authority's policy, standards and procedures are being met.