

ITASS Data Security Guidance

ITASS SIMS Remote Working - USER AGREEMENT

ITASS, in partnership with Synetrix, agrees to setup the configuration of your school server to enable remote access to your school network via a dedicated PC subject to the terms and conditions stated in this user agreement. By signing this agreement and using the Synetrix remote portal to access your school server you are consenting to be bound by, and are becoming a party to, this agreement. Only employees of {School Name} and approved third parties may use the Remote working service. Users of the remote working service are responsible for ensuring it is used in a secure way.

The remote working service is available to all relevant school staff, who have signed a user agreement, subject to approval by the head teacher and the purchase of the necessary licenses. ITASS should be informed, by the head teacher, of any staff who needs to be added or removed to the authorised user group. Under no circumstances should user accounts be disclosed and share amongst colleagues.

HARDWARE & SOFTWARE REQUIREMENTS

It is strongly recommended that the remote working service and the associated Synetrix portal should only be accessed via a dedicated school computer which has been purchased or rebuilt specifically for this purpose. In using the remote working portal a user's PC is a de facto extension of the {School Name} network, and as such are subject to the same rules and regulations that apply to other, school owned, equipment (i.e. must comply with ICT Security and Usage Policies for {School Name}, in addition to the terms of this agreement). As a user of the remote working service you are responsible for the condition of a specific PC (computer name: {PC Name}), which has been setup to access the Synetrix portal, and should ensure that it is fully protected against any computer attack that could compromise its security. By signing this document you agree that the PC, used to access the remote working service, will be configured to meet the following criteria

- The PC should be running Windows XP professional or Windows Vista Business
- The PC should have the latest windows updates installed and should be configured to download and install Microsoft Windows updates automatically.
- The PC should be running up to date anti-virus software and should be configured to download and install updates automatically.
- The Internet browser software should be up to date and the security level should be set to medium-high or high.
- The Windows firewall should be enabled and no exceptions added without consulting ITASS first
- Software that is not essential for school duties should not be installed without first consulting ITASS and obtaining the head teacher's approval. Furthermore, any software installed, by ITASS, as part of the initial laptop setup should not be removed.
- Network traffic entering the school internal network should emanate only from the approved user PC. Whenever practicable traffic emanating from other networks, which may be connected to the PC, should be blocked.
- Access to the remote working portal over a home wireless internet connection is not recommended. Where a wireless connection is unavoidable the WLAN router should be configured to use the most secure standard available. At the very least Wi-Fi Protected Access (WPA) should be used. However, if supported by your laptop and wireless router, it is recommended that WPA2 should be used.

ITASS Data Security Guidance

ACCEPTABLE USAGE POLICY

In addition, by signing this document you agree to use the remote working service in an appropriate and secure manner that meets the following criteria

- Users with remote working privileges must ensure that unauthorised users are not allowed access to any dedicated remote working PC.
- The service is to be used only for activity directly related to {School Name} work.
- Internet access on the PC, not relating to the Synetrix portal, should be kept to a minimum where possible and should always be in accordance with the school's own Acceptable Usage Policy.
- Users must not attempt to access the remote working portal on machines other than the dedicated remote working PC(s).
- All users must agree that they will not compromise confidentiality by attempting to log on to SIMS in public places or any other place where unauthorised persons might see the screen.
- All users agree that they will only print data, originating from SIMS.net or FMS, off site when necessary. In such situations, users agree to only print to equipment located in their own home and to ensure there is no unauthorised access to the printed data. All users must be aware that when printing any school data, if such data is viewed by a third party it could be considered a breach of confidentiality. All users should also take necessary steps to securely store and dispose of such printed material.
- All users agree that they will not save anything to the local disk that they are not prepared to lose. Locally stored documents are not backed up and may be lost if the PC needs to be repaired or rebuilt. To prevent potential data loss, it is strongly recommended that all work is saved to an appropriate location on the school network.
- Users who access the remote working service must use a strong password for their network and SIMS.net accounts. The passwords should be made up of numbers and upper and lower case characters and should be changed on a regular basis.
- All users must agree to keep their log-on username and password private. All users must agree not to disclose their account details to anyone, or leave these usernames and passwords anywhere where they may be seen by others
- Users must take all reasonable steps to make sure that their machine is physically secure when logged in. A PC should be locked and password protected when leaving it unattended.
- All users must agree to always log off correctly, using the 'sign off' button in the Synetrix portal, when they have finished working.
- Users must not try to reconfigure the PC, setup to use the remote working service, in any way that might compromise its security.
- Users must not opt to save their username or password if prompted as part of the login process.
- Users are required to inform the school and ITASS if they no longer require the service and must inform ITASS immediately if a PC, used to access the remote service, is lost or compromised, so that it can be prevented from future use.
- All users are required to conform to the Information Security Policy of The London Borough of Newham (<http://newhamintranet/resources/ict/themes/ituserguidesandpolicies.htm>). The information security policy requires that any information seen by a user, such as that held within the school's information management system (SIMS), must be kept private and confidential EXCEPT when it is deemed necessary by law to disclose such information to an appropriate authority. The policy also governs the printing of such information.

ITASS Data Security Guidance

ITASS uses a remote management tool called Centrastage which can be used by ITASS to monitor the software installed together with the status of the virus software, windows updates and drive space. Any users found to have violated this policy will have their remote access revoked and further disciplinary action may be taken. The school reserves the right to withdraw remote access privileges at anytime with no reason given.

I have read, understood and agree to abide by the terms and conditions of the ITASS SIMS Remote User Agreement.

Name:	Signature:
Date:	

Please return to your Data Manager/Head and return a copy to ITASS

Glossary of Terms

Synetrix portal

A dedicated web access point via the URL {SRA URL} provided by Synetrix, which has been pre-configured to provide a secure connection onto a specific school server

Remote working service

The provision of a dedicated web access point via the Synetrix portal which can be used to open a secure connection between a dedicated PC and the school server allowing locally installed programs such as SIMS.net to access the school server as if the PC was connected to the school network directly.