REMOTE ACCESS POLICY & PROCEDURE

JULY 2013

Author:	**Steve Williams**
Date:	**September 2011**

Agreed:

	EIS
	Management
	Unison

Purpose

The purpose of this policy is to define standards and restrictions for connecting to West Lothian College's (the College) internal network from an external location via remote access technology. The College's resources (i.e. corporate data, computer systems, networks, databases, etc.) must be protected from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to our public image. Therefore, all remote access for College employees must be achieved with minimum risk to the College via standard, audited methods.

Context

College-based systems have until recently been inaccessible from outside the College campus. A remote access solution offers several benefits including:

- what can be accessed (all resources available to a staff member on campus)
- from where it can be accessed (files, email and College systems are now
- accessible from home, from other institutions or via public WiFi services such as in cafes)
- when it can be accessed (anytime, not dependent on College opening hours).

Remote Access

Remote access is defined as any connection to West Lothian College's network from off-site locations, such as the employee's home, a hotel room, airport, café or other institution.

Scope

This policy applies to all authorised College staff members who utilize College or personally-owned computers to remotely access the organisation's data and networks. Employment at the College does not automatically guarantee the granting of remote access privileges.

Any and all work performed for West Lothian College through a remote access connection is covered by this policy.
Work can include (but is not limited to) e-mail correspondence, Web browsing, accessing server-stored files, and any other company application, for example Columbus or Serengeti.

Supported Technology

All remote access connections will be centrally managed by West Lothian College's IT department by encryption and strong password protection. Remote access connections as defined by this policy mean Virtual Private Network (VPN) connections which establish a secure "tunnel" into the College network, over home

Broadband, or via WiFi connections in public places. These VPN connections will be made via the Cisco VPN client ONLY, which will be provided by ICT for installation by staff.

System Requirements

Any member of staff wishing to access College resources via a VPN connection must be able to satisfy ICT Services that they have a PC or laptop with Windows XP or newer (including the latest Windows updates), or a MAC with at least MAC OSX 10.5. Any connection depends on the user having an active Internet connection.

Eligible Users

All staff requiring remote access for business purposes must go through an application process that clearly outlines why the access is required and what level of service the employee needs should his/her application be accepted. Application forms must be approved and signed by the employee's line manager before submission to ICT Services.

Procedures

It is the responsibility of any employee of the College with remote access privileges to ensure that their VPN connection remains as secure as his or her network access within the office. It is imperative that any VPN connection used to conduct West Lothian College business be utilized appropriately, responsibly, and ethically. Therefore, the following rules must be observed:

1. General access to the Internet from homethrough West Lothian College's network is permitted. However, this must not be used for recreational purposes – the remote access connection must be disconnected prior to accessing such Internet sites.

2. Employees must maintain their personal Windows or Mac operating system with current updates to avoid security issues. For more detail on security for devices see the Electronic Information Security Policy suite on Serengeti.
3. Employees will use secure remote access procedures. This will be enforced through Windows passwords (a mixture of upper- and lower-case letters, numbers and extended characters such as '!'). These passwords will also apply when in College.. Employees must not disclose their passwords to anyone, including family members if business work is conducted from home.

4. All remote computer equipment and devices used for business work, whether personal- or college owned must have installed whatever antivirus software is deemed necessary by West Lothian College's ICT Services.

5. Remote users using public areas for wireless Internet access must use a Cisco VPN client which will be provided by ICT Services.

6. ICT Services cannot provide technical support for a home broadband connection, public WiFi connection or other institution connection.

7. WiFi users must disconnect wireless sessions when not in use in order to mitigate attacks by hackers and eavesdroppers.

8. Users must apply new Windows passwords every business/personal trip where college data is being utilized over a WiFi service, or when a college device is used for personal Web browsing (steve does this contradict point 1?). ICT Services will provide instruction on changing passwords should this be requested.

9. Employees with remote access privileges will make no modifications of any kind to the remote access connection without the express approval of West Lothian College's ICT Services.

10. Employees with remote access privileges must ensure that their computers are not connected to any other network while connected to West Lothian College's network via remote access, with the obvious exception of Internet connectivity.

11. In order to avoid confusing official company business with personal communications, employees with remote access privileges must never use non-college e-mail accounts (eg. Hotmail, Yahoo, etc.) to conduct West Lothian College business.

12. No employee is to use Internet access through company networks via a VPN connection for the purpose of illegal transactions, harassment, competitor interests, or obscene behavior, in accordance with the Computer and Email Acceptable Use Policy.

13. All remote access connections must include a "time-out" system. In accordance with West Lothian College's security policies, remote access sessions will time out after 20 minutes of inactivity, and will terminate after 4 hours of continuous connection. Both time-outs will require the user to reconnect and re-authenticate in order to re-enter company networks. Should a remote user's account be inactive for a period of 90 days, access account privileges will be suspended until ICT Services are notified that the account should be reactivated.

14. If a personally- or college-owned computer or related equipment used for remote access is damaged, lost, or stolen, the authorized user will be responsible for notifying their manager and West Lothian College's ICT Services immediately.

15. The remote access user also agrees to report immediately, to their manager and West Lothian College's ICT Services, any incident or suspected incidents of unauthorized access and/or disclosure of company resources, databases, networks, etc.

16. The remote access user also agrees to and accepts that his or her access and/or connection to West Lothian College's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in

order to identify accounts/computers that may have been compromised by external parties.

17. West Lothian College will not pay connection or any other charges for any remote access session.

Any queries relating to any of the above points should be referred to ICT Services.