Removal of user policy

Policy Statement:

An important aspect of maintaining the security and safety of the schools data is to ensure that only users with the correct authorization have access to the data. Computerized user accounts are the means used to grant access to systems and applications. Creating, controlling, and monitoring computer accounts are actions that are critically important to overall security policy and strategy. The purpose of this policy is to provide mechanisms that define and manage accounts for User communities accessing [LEP] resources.

The School has an established and documented process to set up access to the network, state applications (ADEConnect, common logon) and IT services.

1. Users request access that is reviewed and approved their supervisor:
   a. The IT department sets up access to the local network and IT services
   b. The ADE Entity Administrator applies the necessary access to ADEConnect and requests common loon via the ADE helpdesk ticketing system.

This policy aims to ensure that the school has a robust process for the timely removal/disabling of users that have left the School or have changed role for key applications. This should be done in a timely fashion to ensure that there is no risk of unauthorized access to or modification of data. Access should be revoked within 24 hours where possible.

Procedure: It is the responsibility of the employees Supervisor to ensure that access is revoked for staff leaving or changing their responsibility. Supervisors must ensure that processes that are used when staff leave (exit forms, exit interviews, etc) incorporate a check on which systems need to have access revoked. The ADE Entity Administrator will conduct an annual review of users on the systems to ascertain that the correct users have access to the correct user roles.