

ITASS Data Security Guidance

Account Management - Guidance for Secondary Network Managers

Data Access Control

- Decide on what data is sensitive, secure or personal and who needs access to it. This should be done in consultation with the Head Teacher and Senior Management Team (SMT).
- Create Local Groups in Active Directory (AD) to represent the groups of users identified above.
- All users of the network should be assigned to one of these local security groups.
- Create folders that can be used to store the data identified above into categories based on which users need access to.
- Assign access to the folders above based on the local security group.
- Configure AD to enable a password protected screen saver after a limited time out period.

Password Management

- Configure AD to force users to use password complexity
- Store email and log on account details securely in a password protected document within a secure folder. Do not keep paper records of accounts.
- Force periodic password changes
- Force password changes when a security breach occurs or a password disclosure is suspected.
- Configure AD to limit unsuccessful log on attempts in order prevent the guessing of passwords.
- In case of an emergency in the absence of the Network Manager, the administrator account details should be kept securely in a sealed envelope.
- Users who forget their account details should see the network manager in person to effect the resetting of their account.

Leavers and Temporary Staff

- Information system access and privileges should be terminated when the employee's contract ends.
- Network Managers should be informed by admin staff whenever an employee leaves. Network Manager gets the final decision from the head to delete the account.
- All users' personal data should be deleted.
- User accounts should be created with a limited log on period for temporary staff (dependant on the length of contract).