

What to Do When a Teacher Leaves



The purpose of this document is to:

- Help ensure that a school's data and resources remain secure as personnel leave the organisation
- Help reduce the opportunity for misplaced or malicious allegations.

This document could be included in the staff induction pack and used as part of wider staff development programme.

Acknowledgements:
Adapted from material by Kent County Council

Adults who work in schools may have access to a range of important and sensitive information including images and personal details of colleagues and learners and it is essential that the integrity of the school's systems and files remain intact when colleagues leave the school.

- Email – disable password. School technical administrators will need to keep access to the account by forwarding mail to an alternative account. This will help address any ongoing issues, projects that need to be completed, outstanding actions etc.
- Network – change access password. Delete files or inspect prior to making them available to other users.
- Secure areas – ensure key codes are changed and all keys retrieved.
- Portable devices – need to be thoroughly checked for inappropriate content, malware, illegal copies etc. prior to being made available to other users.
- Learning platform – account disabled but not deleted. This will ensure all useful documents can continue to be used by the school.
- Files, programs, data - ensure none are taken away from the school if the copyright is only for the institution.
- Images – no teacher can take images of pupils away from the school when they cease to be employed by the school.

'Shared Accounts – Evaluate the requirement to change any shared service passwords such as administrator accounts on servers, printers and network devices. Additionally, consider the service contracts and web sites where the employee is a named contact.

Start writing your procedure by taking an example employee and creating a list of the devices and systems to which they have access and prioritise these in terms of potential threat and impact.

You may want to consider maintaining a database or spreadsheet of all access levels and devices given to staff, this could then be used as a checklist in the event of a member of staff leaving.'

www.eiskent.co.uk

The technical to do list

Disable/delete Active Directory user account - A decision must then be made relating to the files and programs on the user's home drive.

Change Wireless encryption keys whenever a colleague ceases to be a member of staff.

Regularly check Active Directory for unused or spurious user accounts, unusual activity and disable.

Ensure encrypted data is unencrypted or deleted when user leaves.

Learning Platform accounts disabled/deleted and resources archived/deleted.

Modify user account password in the event that you may need to access in future. This should be documented in the appropriate acceptable use policy.