

TUESDAY'S LIVE TOP TIP



OUR WEEKLY DOSE OF SMART BUSINESS AND FINANCE TOP TIPS



Check leavers' system access is removed promptly

Why?

Reduce Security Risk

- Remove access to email, finance, HR, safeguarding and other systems promptly.
- Recover devices, passes, keys and other access credentials.

Protect Your Data

- Former staff should not retain access to confidential information.
- Include third-party systems and cloud applications in your leaver checklist.

Useful Resources

- NCSC – Managing User Access
- DfE – Cyber Security Standards

Benefit

Promptly removing access when an employee leaves reduces the risk of unauthorised access to personal, financial and confidential information. A good leaver process should cover all systems, not just email, including MIS, finance, HR, safeguarding platforms and cloud services. Using a documented checklist provides assurance that access has been removed consistently and reduces the risk of dormant accounts being compromised or former staff retaining access to organisational information.