Starters, movers, and leavers; a cyber defence policy

Date of policy (month and year)

UNIVERSITY OF WINCHESTER

Document Title:	*University staff starters, movers and leavers and the cyber defence requirement policy*
Document Author:	Fiona Greig
Responsible Person and Department:	Fiona Greig Knowledge & Digital Services
Approving Body:	University Leadership Team
Date of Approval:	26th July 2023
Date Effective From:	*July 2023*
Review Date:	***31st July 2026***
Indicate whether the document is for public access or internal access only Indicate whether the document applies to collaborative provision? *(Strikethrough text, as appropriate)*	**Public Access** **Applies to Collaborative Provision**

Summary:

One of the key defences to cyber attack, and innappropriate data access, is to ensure that access to University systems, solutions and equipment are managed appropriatly and that line managers take responsibility for ensuring that communications and applications for access are activly managed.

There is opportunities to transform the onboarding process for staff and students and KDS are keen to work with process owners. But this policy covers the existing processes.

This policy outlines the expectations for the lifecycle of all University "staff" account holders.

TABLE OF CONTENTS *(right-click table below and select 'Update Field' and, if given option, 'Update entire table').*

1. Applicability

1.1. This policy allies to all non-student account holders who are provided access to our University systems. Including but not limited to:-

1.1.1. Permanent staff members

1.1.2. Temporary staff on fixed-term contracts

1.1.3. Casually employed staff (e.g. KDS support team, student ambassadors…)

1.1.4. Visiting Lecturers

1.1.5. External Examiners

1.1.6. Members of the Board of Governors

1.2. The policy covers the initiation of an account.

1.3. Duties expected of line managers as people move between roles within the University

1.4. Actions to be taken as a staff member leaves our employment, in both planned and unplanned circumstances.

2. New starters

2.1. Once a contract is agreed, and confirmed by Human Resources, there are a number of activities that line managers are responsible for:-

2.1.1. Requesting a new IT account stating starting date (Servicedesk request)

2.1.2. Requesting any required hardware stating starting date (laptop, mobile phone, etc..), specialist software and "telephone landline" requirements (Servicedesk request)

2.1.3. Outlining what permissions their role requires on corporate systems e.g. SITS, Unit4ERP, and if there will be any remote working the deployment of the Citrix client with the list of applications that the line manager requires the role to be able to utilise while off-campus. (ServiceDesk request)

2.1.4. Recruiting managers will ask for a digital photo of the new colleague. They will then forward to ServiceDesk with the colleague details requesting a new staff card is printed using attached photo and stating starting data (ServiceDesk request)

2.2. On the persons first day on Campus the line Manager will ensure the new team member visits the Knowledge & Digital Services desk in the Martial Rose Library to allow collection of all equipment, their card and to ensure the new starter is comfortable with getting started.

2.3. Account requests should be created at least 3 days before the colleague is due to start.

2.4. Occasionally some roles request early access to their IT accounts. This can be facilitated by KDS but this should happen only in exception and normally for senior roles only and authourised by Director of Knowledge & Digital Services.

3. Members of staff moving roles

3.1. If a staff member is leaving their role the ***existing*** line manager is responsible for:-

3.1.1. Informing KDS of the date the colleague is no longer going to be part of the team, this allows us to update central distribution and permission lists.

3.1.2. Outline the systems and permissions the team member no longer requires from that date – you should not assume their new role requires anything.

3.1.3. Manually remove the colleague from all locally managed distribution lists, shared file locations and any local Teams.

3.1.4. Inform KDS that the staff member is taking their University managed laptop with them into their new position.

3.1.5. Where specialist IT is required for the role this should be handed back to the line manager, as should any University mobile phone.

3.2. The ***new*** line manager should:-

3.2.1. Request permissions for their new starter in line with what their role requires on corporate systems e.g. SITS, Unit4ERP, and if there will be any remote working the deployment of the Citrix client with the list of applications that the line manager requires the role to be able to utilise while off-campus.

3.2.2. Requesting any required hardware stating starting date (laptop, mobile phone, etc..), specialist software and "telephone landline" requirements.

4. Members of staff leaving the University / end of contract

4.1. When a team member has agreed their leaving date the line manager should inform KDS, This email should also outline any permissions that the person has on any corporate systems. Ideally this should happen at least 3 days before end of contract, however where people leave the University without notice KDS should be informed immediately.

4.2. On the last day of the team member the line manager must retrieve:-

4.2.1. University card – this to be returned to KDS for secure disposal.

4.2.2. University Managed laptop – this to be returned to KDS to allow any additional clean-downs and upgrades.

4.2.3. University issued mobile phone – this to be returned to KDS.

4.2.4. Return of any University equipment where permission to remove to facilitate working at home has been granted – this to be returned to KDS for redeployment.

4.2.5. Any locally issued equipment or storage devices – these to be retained by the Faculty / Department for future deployment.

4.2.6. Any specialist or Faculty/Department issued equipment – this to be retained by the Line Manager / Administration Office for future deployment.

4.3. People cannot request continued access to "their" files or emails. They should remove anything personal before they leave and if there are any files/emails retained in their personal locations these must have been moved before the end of contract. Any documentation (files, emails, images) etc that have been stored in personal email, Desktop or OneDrive areas must be transferred to managers before the last date of employment. Managers are not able to access content once an employee leaves as the account will be deleted.

4.4. These steps must be followed, even if there are aspirations for the individual to work for the University again. If permission to extend a contract or issue a new contract has not been received at least three days before someone is due to leave their account will be removed. ***This will happen at 17:00 on their last day.***

5. Failure to comply with this policy

5.1. Not managing access to University systems is a major compromise of our cyber defences. Anyone failing to follow these procedures may face formal disciplinary proceedings.

5.2. Where University equipment is not retrieved from team members by their last day the Dean/Director will immediately be informed and will be charged for the replacement of that equipment.