PennPrivacy
Office of Audit, Compliance & Privacy

Privacy Office Offboarding Checklist – Supervisor/Manager

When you become aware that a Penn employee will be leaving their position, it is important to understand all systems, records and data to which the employee has access to or otherwise maintains as a function of their position at Penn.

You should discuss the transfer of all such information and/or access to systems with the employee and your Local IT Support Provider (LSP). You should ensure that the employee no longer has access to Penn systems or other records or data (in physical or electric form) including, but not limited to, individual personal data or student education records.

In order to facilitate these discussions, the Privacy Office has created the following checklist for you to complete while offboarding the employee. You will need to undertake the following Privacy Office Offboarding Tasks in the weeks leading up to the employee's departure date.

You should use this checklist to work with the employee to identify all substantive data and records and who should have access to them in order to establish a plan ensuring a seamless and secure transfer occurs before the employee's departure date.

Before the employee leaves Penn, you should have them sign the Privacy Office Offboarding Checklist – Employee. You should keep the signed Privacy Office Offboarding Checklist – Employee, along with your signed copy of the Privacy Office Offboarding Checklist – Supervisor/Manager, in departmental files in the event it is needed for future reference.

For more detailed guidance on the disposition of documents when staff leave the University, please refer to the Disposition of Documents Guidance.

Manager’s Offboarding Tasks to Be Completed 1-2 Weeks Before Employee Departure	Yes	No	N/A
1. **Offboarding Checklist to Employee** Did you provide the ***Privacy Office Offboarding Checklist – Employee*** to the employee at least two weeks prior to their last day of employment at Penn?			
2. System Access Did you review with the employee all Penn systems or third-party platforms which the employee has access to or maintains accounts, files, folders, or information? You should review with the employee those systems that the employee has identified in the ***Privacy Offboarding Checklist – Employee*** (See Questions #1-#7)			
3. Deprovisioning Employee Access For each system the employee identified in the ***Privacy Offboarding Checklist – Employee***, have you coordinated with your LSP termination of the employee’s access?			
4. **Transfer of Access to System Files** If Penn needs continued access to the employee’s files/folders in any of these systems, have you consulted with your LSP to arrange for the transfer of those files – particularly those files/folders for which the employee is the designated owner?			
5. **Employee Data Inventory and Disposition** Did you work with the employee to inventory the documents and data that the employee has developed and maintained as a function of their role to determine the appropriate method of disposition of the documents? You will need to consider whether to maintain, transfer, archive and/or purge the data, while also complying with Penn’s data retention requirements. *See https://archives.upenn.edu/records-center/*			
6. Transition Memorandum Did you review the employee’s transition memorandum of potentially open and/or ongoing projects and discuss the location of data relating to those projects?			
7. **Research Grant Data** Does the employee work on research grants? If so, Penn’s Office of Research Services must be informed of the departure of the employee and must be consulted to determine, for example, whom to notify (e.g. the Principal Investigator, the sponsoring agency) and in general to address the handling of the data.			

8. Penn Data on Personal Devices Does the employee have any Penn data on a personal device(s)? If **yes,** consult with your LSP on how best to coordinate with the employee to delete all electronic files containing University data, and University licensed software on the personal device.			
9. **Paper/Electronic Files at Home** Does the employee maintain any paper/electronic files at home that contain University data?			
If **yes,** has the employee returned them to the office and are you aware of the nature of the documents and their location?			
10. **Personal Email Account** Did the employee forward their Penn emails to a personal email account? If **yes**, direct the employee to work with your departmental LSP to delete all Penn-related files containing University data			
11. Student Education Records Did you confirm with the employee that they do not maintain in their possession any student education records? All student education records shall remain in the possession of Penn**.**			
12. **Litigation Holds** Are the employee's records currently subject to a litigation hold? If **yes**, consult with the Office of General Counsel regarding the handling of those records.			
13. **Schedule Meeting with Employee** Have you scheduled a meeting with the employee to review their responses to the ***Privacy Office Offboarding Checklist – Employee***?			
Manager's Offboarding Tasks To Be Completed Before Employee Leaves	**Yes**	**No**	**N/A**
1. Technical Property Did the employee return all technical property back to Penn? This includes, but not limited to, laptop, laptop accessories (case, AC power adapter, mouse, keyboard), desktops, flash or USB drives, and mobile devices.			
2. Physical Access Did the employee return all physical access devices? This includes employee's PennCard, office key, desk key, and/or cabinet key. *NOTE: If employee is transferring to another Penn department, the employee should keep their PennCard.*			

3. Corporate Card(s) Did the employee return his or her corporate card(s)?			
If **yes**, did you properly destroy and dispose of the card?			
4. Student Education Records Did you confirm with employee that no student education records remain in their possession? All student education records shall remain in the possession of Penn**.**			
5. Penn Personal Data Did you confirm with employee that no individual's personal data that the employee had access to by virtue of their position with Penn remains in their possession?			
6. Licensed Software Did you confirm with the employee that all licensed software on personally owned computers and mobile devices has been uninstalled? If not uninstalled, consult with your LSP to uninstall Penn licensed software.			
7. Personal Items Is the employee's workspace clear of all personal items?			
8. Web Content Did you contact the departmental webmaster to ensure references to employee are removed from web content?			
9. Meeting Invites Did you remove the employee from recurring meetings in Outlook as an attendee?			
10. Systems Access – Did you verify that employee access to Penn systems and any other systems identified in the ***Privacy Offboarding Checklist – Employee*** (See Questions #1-#7) has been terminated?			
11. Governmental Systems Access - Did you verify removal of employee from accessing any governmental systems?			
12. Executed Offboarding Checklist - Did you receive a signed ***Privacy Office Offboarding Checklist – Employee*** from the employee prior to the employee's departure?			

___________________________ ____________________________________ __________________

Supervisor/Manager Name Signature Date