

 Weill Cornell Medicine	WCM Administrative Policy and Procedure	
	Policy Title	Directory
	Policy Number	ITS-500.13
	Department/Office	ITS Security
	Effective Date	July 17, 2015
	Last Reviewed	September 11, 2024
	Approved By	WCM-Executive Policy Review Group
	Approval Date	October 21, 2025

Purpose

All members of the Weill Cornell Medicine (WCM) community are responsible for maintaining a Directory profile which contains accurate, updated, and relevant information about their positions.

Scope

This policy applies to all WCM Workforce Members who utilize WCM information technology resources as well as those responsible for managing and safeguarding WCM data.

Policy

All members of the WCM community are responsible for maintaining a Directory profile which contains accurate, updated, and relevant information about their positions.

Definitions

Workforce Members: Any Faculty; Staff; Students; Volunteers; Trainees; and other persons whose conduct, in the performance of work for WCM, is under the direction and control of WCM, whether or not they are paid by WCM.

Procedure

The Directory is an aggregate of contact information from various systems of record at WCM. The Directory is accessible online at <https://directory.weill.cornell.edu>. Various data attributes are visible depending on the publication settings within a user's profile.

The Directory contains information about the following types of active people:

- 1) employees at WCM and WCM-Qatar,
- 2) faculty and non-faculty academics at Weill Cornell Medical College and the WCM Graduate School of Medical Sciences,
- 3) students, although published information may be limited due to the Family Education Rights and Privacy Act (FERPA), and
- 4) affiliates, including, but not limited to, Cornell University (Ithaca), NewYork-Presbyterian Hospital, Hospital for Special Surgery, or volunteers.

The Directory is populated from a variety of systems as listed below:

- Academic Staff Management System (ASMS) – the system of record for faculty
- Weill Business Gateway (WBG) – the system of record for employees
- Physician Organization Profile System (POPS) – a system for tracking clinical contact information
- Jenzabar – the system of record for students
- MARIA – the system of record for affiliates, such as vendors, contractors, and other temporary staff
- Avaya – the system for tracking WCM-issued phone numbers
- Non-Employee Management System (SharePoint) - the system for tracking volunteers

Most data attributes in the Directory can be set to different visibility levels as described below:

- Public – viewable by anyone (e.g. accessible to the internet)
- WCM – viewable by members of the WCM community, either while on the campus network or while logged in to the Directory
- Department- viewable by members of the individual's primary department while logged in to the Directory
- Emergency – not otherwise viewable, except for emergencies or identity verification

1. Individual Responsibilities

To ease and facilitate communication among the institution, all WCM employees must publish current contact information in the Directory.

1.01 Accuracy of Information

All members of the WCM community are responsible for maintaining the information contained within their profile. Contact information should be updated at least annually or sooner if phone number, email address, or location changes.

1.02 Preferred Name

Anyone may choose to identify themselves within the WCM community with a preferred first and middle name that differs from their legal first and middle names.

Legal names are maintained in the appropriate systems of record. Legal names appear in employee records (e.g., payroll documents), student records (e.g., financial aid documents, official transcripts, diplomas), federal requests for information, academic certifications, and federal immigration documents.

Preferred names are maintained in the Directory and appear in Microsoft Outlook, Microsoft Teams, and other downstream systems that utilize Directory data, including building security badges. Preferred names may not be used for purposes of fraud or misrepresentation. WCM reserves the right to remove a preferred name if it contains inappropriate or offensive language or violates WCM policies.

1.03 Preferred Pronouns

Anyone may choose to identify themselves within the WCM community with a preferred pronoun. Preferred pronouns can be published publicly or just to the WCM community. Preferred pronouns are maintained in the Directory and appear in downstream systems that utilize Directory data (such as Office 365). Preferred pronouns will not automatically appear in one's email signature.

1.04 Required Visibility of Phone Numbers

All WCM employees must have at least one phone number published to WCM (preferably the employee's direct number and/or a department number).

All exempt employees and faculty must have at least one phone number published to Public (preferably the employee's direct number and/or a department number). This does not apply to non-FLSA exempt employees.

1.05 Required Visibility of Email Addresses

By default, email addresses issued by WCM will be published to *Public*. At the employee's discretion, they may reduce the visibility of their WCM email address to the WCM community by publishing it to *WCM*.

Individuals with email addresses issued from a WCM affiliate (as officially maintained on the WCM website) may be published to *WCM*. These affiliate addresses may be published to *Public* at the discretion of the individual in compliance with the affiliate institutions' policies. Only email addresses ending with @med.cornell.edu, @qatar-med.cornell.edu, @cornell.edu, @nyp.org, @hss.edu, or @mskcc.org can be published to *WCM* or *Public*. Only these email addresses can be set as the individual's primary email address.

Personal email addresses or other professional email addresses not ending in one of the above domains may only be published to Department or Emergency. ITS policy 500.08 – *Use of Email* must be respected for appropriate communication.

1.06 Required Visibility of Locations

All WCM employees must have a location published to *Public*. Valid locations are available from the Directory drop-down menu.

1.07 Required Submission of Emergency Contact Information

WCM maintains "Weill Cornell Alert" to provide emergency information and instructions. Weill Cornell Alert can send simultaneous notifications to the WCM community via:

- Cell phone (voice and SMS text messaging)
- Home phone
- Work phone(s)
- Alternate phone(s)
- Home and work email(s)
- Pager
- Fax

All WCM faculty, staff, and students are required to add their emergency contact information in their Directory profile (using the *Emergency* drop-down option) to be added to the Weill Cornell Alert system. This information will not be displayed on your Directory profile as it will only be used by the automated emergency notification system.

1.08 Student Visibility

As specified by the Family Educational Rights and Privacy Act (FERPA), students have the right to opt out of displaying their record in the Web Directory. Students who opt out via FERPA can do so in Jenzabar through LEARN, and will not be visible in the Web Directory, even to logged-in users. In cases where a student also has an exempt employee role, only the student role will be hidden, as opposed to the entire person record.

1.09 Appropriateness of Photographs

All WCM employees are encouraged to publish a professional business headshot to the Directory. Published photographs will synchronize with Microsoft Outlook, Microsoft Teams, and other downstream systems that use Directory data. Photographs must include the face, head, and shoulders in a plain background not cropped too closely to the head. Photographs must be in color and of an acceptable resolution (minimum of 200 x 200 pixels and 72 DPI).

To qualify as a profile picture on the Directory, individuals should be posed and in professional attire. Selfies, pictures taken with a cell phone, and action or candid shots (such as sitting at a desk, giving a talk, or during a meeting) might not be acceptable and are subject to removal.

2. Additional Resources

The following additional resources are available:

[Emergency Notifications](#)

[Weill Cornell Medicine Affiliations](#)

Compliance with this Policy

All WCM Workforce Members are responsible for adhering to this policy. Failure to comply will be evaluated on a case-by-case basis and could lead to corrective action, up to and including termination, consistent with other relevant WCM and University Policies. Instances of non-compliance that potentially involve a lapse of professionalism may lead to engagement of the Office of Professionalism for evaluation and intervention.

Contact Information

Direct any questions about this policy, ITS-500.13 – *Directory*, to the Office of the Chief Information Security Officer, using one of the methods below:

Office: (646) 962-3609

Email: ciso@med.cornell.edu

References

WCM Policy ITS-500.08 – Use of Email

Policy Approval

This policy was reviewed and approved by:

- Information Security and Privacy Advisory Committee (ISPAC) on September 18, 2025.
- WCM-Executive Policy Review Group (WCM-EPRG) on October 21, 2025.

Version History

Date	Author	Revisions
07/17/2015	Brian J. Tschinkel	Policy implemented
12/10/2019	Brian J. Tschinkel	Specified email domains which can be set as primary
08/03/2022	Brian J. Tschinkel	Modified required minimum visibility of primary email address
08/29/2023	Brian J. Tschinkel	Updated policy template and language to conform with branding
07/30/2024	Tom Horton	Updated contact information and some general language updates
09/11/2024	Tom Horton	Updated policy template and added FERPA visibility section
10/21/2025	Office of the CISO	Updated policy template, removed requirement for recent photographs and removed reference to ITS photography services

Appendix

N/A