POLICY

Purpose

To uphold institutional data security standards while maintaining appropriate access to employee contact information for internal and external communications.

Policy Statement

In support of the College's commitment to cybersecurity and responsible data management, the following practices govern the publication of employee directory information:

1. Public Website Directory:
    - The College's public-facing website will not display individual employee email addresses to mitigate risks associated with spam, phishing, and unauthorized data harvesting.
    - General departmental email addresses will be provided only for departments that require direct interaction with the public. These addresses will serve as the primary point of contact for external inquiries.
    - Employee names, titles, and office locations may be listed publicly, but individual contact details will be excluded.
2. Internal Directory (Intranet):
    - A complete employee directory, including names, titles, office locations, phone numbers, and email addresses, will be maintained on the College's secure intranet.
    - Access to this directory is restricted to authorized users through secure login credentials.
3. Governance and Oversight:
    - Decisions regarding the publication of directory information are made at the discretion of the College, in accordance with institutional security protocols and operational needs.
    - This policy will be reviewed annually by the College's Information Technology and Administrative Services teams to ensure alignment with evolving security standards.

ADOPTED: November 6, 2025