The Responsible Use of Faculty & Staff Data

The Responsible Use of Faculty and Staff Data

This document is a consolidated resource for information on the principles and specific guidelines governing the release and use of data and information about University of Virginia Academic Division, Medical Center and College at Wise employees.

I. Summary

If you have access to HR data, reports, analytics, or dashboards, keep the following guidelines in mind:

1. As a public institution, certain information on our employees must be made available upon request by third parties under the **Virginia Freedom of Information Act.** All such requests must be routed through the FOIA Office. To learn more visit https://foia.virginia.edu/.
2. **Personal identifiers and contact information** including but not limited to name, birthdate, personal home/email addresses, degrees held, visa information, dependents, and marital status are not released to **third parties** unless such entity is contracted by the University to provide a service such as health benefits, life insurance, etc.
3. **Personal identifiers and contact information** are provided **for internal or affiliated business use** only when a justifying use case is approved by the appropriate VP or Dean.
4. **Individual record level data with personal identity characteristics** for legitimate business use cases must have clear data protection, transformation, distribution, retention, and destruction plans to ensure individually identified data is not used in a way that compromises the data privacy standards set by policy.
5. **Demographic data** including Race/Ethnicity, Under-represented Minority (URM) Status, Sex/Gender, Age, Visa Status, Veteran Status, and Disability Status should typically only be analyzed and released in aggregate. Data should not be reported if the cell size is less than 5 members (except in the case of a value of 0 when applicable).
6. **Disability status** is often considered "health information." There are no cases, except for those required by law, where name, title, or other personal identifiers should be reported with this information.
7. **Gender identity and sexual orientation** data will never be released or used in a format other than an overall population figure at the Institution or School/VP area levels unless approved by EOCR/ODE.
8. **URM (Under-represented Minority) status** requests should be clarified with the requestor as different federal agencies or accrediting bodies may have different definitions of this umbrella term. This term can also vary significantly based on context.
9. Requests from internal users seeking **individual or aggregate level workplace related data** such as salary information, tenure, length of employment, job titles, area/unit, etc. can be provided with the employee name field if no personal identity characteristics are also available in the data release.
10. Requests for **business contact information (work emails or phone numbers)** must have a legitimate business justification and should not be requested based on a demographic characteristic *unless the individuals have given free, prior, and informed consent to be contacted for a specific purpose that aligns with the documented request.*
11. Requests to share certain **confidential employee records** with third parties (including other departments at UVA), including but not limited to performance evaluations, disciplinary actions, records concerning grievances or complaints, and Workers' Compensation claims, should not be shared without the employee's express written permission. The employee can consent in writing to sharing the records or may share them on their own behalf.

II. Principles of Use

a. Allowable Purposes

The University accesses, analyzes or otherwise uses employee data in accordance with applicable laws, regulations, and professional standards of practice, and solely for purposes of business necessity in furtherance of the University's mission, goals, and accountabilities. Allowable purposes are determined in compliance with IRM-012 by the President or their delegated representatives, such as Vice-Presidents and Deans.

These purposes often include, but are not limited to:

- Workforce and academic planning
- Diversity and Inclusion analysis
- Cost analysis and budgeting
- Operational analysis and quality assurance
- Grants and contracts administration
- Individual and organizational performance improvement
- Business communications and networking
- Accreditation
- Required federal, state, and other reporting

b. Individual Privacy

Individual privacy, confidentiality and, whenever possible, anonymity, is a top priority. Accordingly, the University does not knowingly or purposefully access, analyze, or otherwise use personal employee data that was shared by an individual with a reasonable expectation of privacy without the knowledge or consent of said individual *except in circumstances where necessary to meet a legitimate business need or comply with legal and/or regulatory requirements* (IRM-012).

Further, the University ensures that it will: **1)** Limit data use to the minimum necessary; **2)** Not attempt to knowingly and purposefully re-identify de-identified data, and; **3)** Make all reasonable efforts to prevent any unlawful and unjustified re-identification.

c. Data Security

- The University ensures reasonable and appropriate technical and organizational safeguards are in place to prevent unauthorized disclosure or breach of data (IRM-003).
- The University employs stricter standards of care when assessing the risk of disclosure, accessing, or otherwise using sensitive data as defined by state law and records management (UDPS 3.0).
- Data used for operational needs or reporting requirements may only be stored for the duration necessary to complete the associated task. Any further retention must be justified (IRM-017).
- The University requires that external entities to which data is released comply with relevant law, data privacy, and data protection standards.

III. Risk Assessment and Mitigation

A risk assessment must take place for any new or substantially changed data release and/or use, whether for internal or external entities. The University must then implement any risk mitigation processes found appropriate and necessary. When assessing the risks of data use and release, consideration must be given to ensure the potential harms to individuals and groups are not excessive in relation to the potential positive impacts.

a. Specific Risk Assessment Guidelines

1. As a public institution in Virginia, the University must make certain employee information available upon request by third parties (external entities) under the Virginia Freedom of Information Act (https://foia.virginia.edu/). **Importantly, however, there are limits on the data that external entities may receive.** Data and information that is already made publicly available through other means will be provided to external entities (such as the press) upon request. Individual employee level data will not be released externally unless required by law.

   When an external request for data originates from an individual or entity without an established data sharing agreement with the University, it should be referred to the FOIA office to review the appropriateness of the request.

2. Personal identifiers and contact information such as name, birthdate, personal home/email addresses, degrees held, visa information, dependents, and marital status are not released to third parties unless such entity has been contracted by the University to provide a service (such as health benefits, life insurance, etc.) or as required by law, and the appropriate approvals are documented in writing.

3. Individual record level data in fields related to various personal identity characteristics (Race/Ethnicity, Under-represented Minority (URM) Status, Sex, Gender Identity, Age, Visa Status, Veteran Status, and Disability Status) will be released solely for legitimate business use cases, and only after clear data protection, transformation, distribution, retention, and destruction plans have been established and documented in writing.

   Data analysts within schools or units who have been authorized by a data steward may be provided access to detailed individual record level data for analysis, however unless an exception has been granted by a data steward, this data should only be shared or released to others only in aggregate. Population sizes under 5 individuals should be suppressed when combinations of primary and secondary identifiers (dimensional context) could be easily combined with other public/semi-public data sets to expose an individual's identity.

   In terms of use, this data may legitimately be used for trend analyses. Demographic data should not be utilized in use cases that involve decision-making at the individual level.

Specific Risk Assessment Guidelines (continued)

4. When requested for internal use to aid in decision-making, individual or aggregate level workplace related data such as salary, tenure, length of employment, job titles, area/unit, etc. which include the employee name field is only provided absent personal identity characteristics such as age, race and gender.

5. Business contact information included work emails or phone numbers is only released for legitimate business purposes. This information will not be provided based on a demographic characteristic unless the individuals have given free, prior, and informed consent to be contacted for a specific purpose that aligns with the documented request.

6. Research using employee data is considered Human Subjects Research and generally requires, at a minimum, Internal Review Board (IRB) approval. However, IRB approval is not necessarily sufficient in and of itself. In addition to the guidelines outlined herein, data requests for the purposes of research are evaluated based on the potential for any findings to be actionable and/or to add to a particular knowledge base or if the timing of a survey request may conflict with other outreach to employees.

7. Unless noted otherwise, data files are approved for one-time use only and are not to be stored or reused beyond the standard retention period or lifecycle of the documented use case.

In addition, the following specific guidelines apply:

Field	Guideline
Disability Status	Disability status is "health information," and will not be released in association with name, title, or other personal identifiers.
Gender Identity and Sexual Orientation	These fields will not be released or used in a format other than an overall population at the Institution or School/VP area levels except as approved in writing in advance by EOCR/ODE*. As such, these fields are not released for purposes of determining salutations/honorifics.
URM (Under-represented Minority)	Underrepresentation is context dependent and must be defined for each use case. Any use of the URM designation should be coordinated and reviewed by the University's EOCR/ODE*.

IV. Procedure: How to Submit Data Requests

a. Submission

Requests should be submitted to the following entities as follows:

Office	Use cases
FOIA Office	Requests from the press or other external/3rd party entities should be directed to submit their requests through the FOIA office.
Institutional Research and Analytics (IRA)	If the use case involves longitudinal data and analytics, the request should be submitted to your local data analytics office or IRA. *More specific examples include* - Workforce and academic planning - Cost analysis and budgeting - Grants and contracts administration - Accreditation - Required federal, state, and other reporting - External Requests for Data (Press, Students, Surveys)
University Human Resources (UVA HR)	If the use case is more operational and real-time, the request should be submitted to UVA HR. *More specific examples include:* - Operational analysis and quality assurance - Individual and organizational performance improvement - Business communications and networking

b. Format and Contents

All requests must include:

- A statement of purpose (the legitimate business use case)
- A description of the data, including the fields & level of aggregation.
  - Data should be requested at the highest level of aggregation possible.
  - Err on the side of specificity when describing what is needed.
- A description of how the data will be stored and used

The following special circumstances require additional information and/or documentation:

- If requesting personal contact information, approval from the University Vice President or Dean to which the institutionally related affiliate is most closely connected.
- For reporting to an external government agency (State or Federal), include the reporting form to be submitted and/or a link to a government agency's description of the request. For information submitted on a form with an approved OMB#, supporting information for grant/contract submissions, and other Federal/State reporting forms may be filled.

  - Forms should be aggregated by an authorized data user or steward and only submitted to the requesting School or Department in a disaggregated/unformatted version if the requestor is an authorized data steward or data user for this area.

- For reporting to an external accrediting agency, include the reporting form to be submitted. Forms should be aggregated by an authorized person and only submitted to the requesting School or Department in a disaggregated/unformatted version if the requestor is an authorized person for this area.
- When requesting data for research purposes, IRB Approval is required, and the requester must submit a PDF of the full and entire IRB application and the IRB Approval of the application.

V. Related Policies and Guidance

If any part of this document conflicts with official University policy, then the University policy must be followed.

IRM-003 Data Protection of University Information
IRM-006 Mass Electronic Mailings
IRM-007 Electronic Mailings for Advancement Activities
IRM-012 Privacy and Confidentiality of University Information
IRM-017 Records Management
UDPS 3.0
HRM-009 Preventing and Addressing Discrimination and Harassment
IRB-SBS
IRB-HSR
UVA-FOIA
DHRM Personnel Records 6.05
UVA Rewards and Recognition
University Data Protection Standards (UDPS 3.0)

VI. Terminology

EOCR/ODE - The University's Office for Equal Opportunity and Civil Rights/Office for Diversity and Equity.

Legitimate Business Use
In principle, the idea of "legitimate business use" is flexible and could apply to a variety of circumstances. In order to determine whether or not there is a legitimate business use, the following considerations will be applied:

- What is the use case? How does it serve the interests and mission of the University and the broader community that the University serves?
- Is it necessary...:
  - for fulfilling the University's mission
  - in order to fulfill a contract
  - for purposes of legal compliance
  - for carrying out a task that is in the public interest

- To the degree that the use will impact an individual's rights and/or expectations to confidentiality or anonymity, does the interest of the University or broader community override those expectations and/or rights?
    - *Individuals may have a reasonable expectation of confidentiality in relation to data fields that apply to them as a person (ex. age, sex, birthdate, home phone number, etc.). This same expectation of confidentiality would not typically apply to information that is related to an individual's job or position (ex. job title, hire date, department, employment status, etc.)*

This document was created through collaboration of the Office of Institutional Research & Analytics, University Human Resources, the Office of the Executive Vice President & Provost, and the Office for Equal Opportunity and Civil Rights.

To find the current version of these guidelines, please refer to the Data Governance resources at www.DataGovernance.Virginia.edu.

Questions about these guidelines may be sent to DataGovernance@virginia.edu.