



Intern Name: \_\_\_\_\_

**PA WIC Dietetic Internship  
Pre-Orientation Requirements Checklist  
(DICAS Applicants)**

(Due June \_\_\_\_, 20\_\_)

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

- PA WIC DI Handbook Acknowledgement Form
- Code of Ethics Acknowledgement Form
- PA WIC Confidentiality Acknowledgement Form
- PA IT Acknowledgement Form

Affiliation Agreements for:

- Community
- Clinical
- Food Service

Completed Preceptor Applications for:

- Community
- Clinical
- Food Service

Intern Agreement (signed between agency & intern)

Non-refundable Tuition Payment Enclosed

Checks, money orders or cashier's check made out to:

**Commonwealth of PA; Bur of WIC**

New Criminal Background (PSP, Child Clearance, FBI) (original copy)

Completed Pre-Orientation Requirements Checklist

Photo Proof of the following:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

- Valid Driver's License
- Valid Automobile Insurance
- Proof of Immunizations (Measles, Mumps, Rubella, MMR)
- Physical Examination from Personal Physician (Stating no limitations)
- Hepatitis B (Proof of 1<sup>st</sup>, 2<sup>nd</sup> & 3<sup>rd</sup> shot) (if applicable)
- Annual PPD (within 3 months of start date)
- Proof of Student AND membership
- Proof of health Insurance
- Drug Tests (if required)
- Valid Serve Safe Certificate
- Professional Liability Insurance to practice Dietetics

Please forward in a sealed manila envelope to:

**PA WIC Dietetic Internship  
DOH/ Bureau of WIC  
625 Forster Street  
7 West, Health & Welfare Building  
Harrisburg, PA 17120**

**Preamble:**

When providing services, the nutrition and dietetics practitioner adheres to the core values of customer focus, integrity, innovation, social responsibility, and diversity. Science-based decisions, derived from the best available research and evidence, are the underpinnings of ethical conduct and practice.

This Code applies to nutrition and dietetics practitioners who act in a wide variety of capacities, provides general principles and specific ethical standards for situations frequently encountered in daily practice. The primary goal is the protection of the individuals, groups, organizations, communities, or populations with whom the practitioner works and interacts.

The nutrition and dietetics practitioner support and promotes high standards of professional practice, accepting the obligation to protect clients, the public and the profession; upholds the Academy of Nutrition and Dietetics (Academy) and its credentialing agency the Commission on Dietetic Registration (CDR) Code of Ethics for the Nutrition and Dietetics Profession; and shall report perceived violations of the Code through established processes.

The Academy/CDR Code of Ethics for the Nutrition and Dietetics Profession establishes the principles and ethical standards that underlie the nutrition and dietetics practitioner's roles and conduct. All individuals to whom the Code applies are referred to as "nutrition and dietetics practitioners". By accepting membership in the Academy and/or accepting and maintaining CDR credentials, all nutrition and dietetics practitioners agree to abide by the Code.

**Principles and Standards:****1. Competence and professional development in practice (Non-maleficence)**

Nutrition and dietetics practitioners shall:

- a. Practice using an evidence-based approach within areas of competence, continuously develop and enhance expertise, and recognize limitations.
- b. Demonstrate in depth scientific knowledge of food, human nutrition and behavior.
- c. Assess the validity and applicability of scientific evidence without personal bias.
- d. Interpret, apply, participate in and/or generate research to enhance practice, innovation, and discovery.
- e. Make evidence-based practice decisions, taking into account the unique values and circumstances of the patient/client and community, in combination with the practitioner's expertise and judgment.
- f. Recognize and exercise professional judgment within the limits of individual qualifications and collaborate with others, seek counsel, and make referrals as appropriate.
- g. Act in a caring and respectful manner, mindful of individual differences, cultural, and ethnic diversity.
- h. Practice within the limits of their scope and collaborate with the inter-professional team.

**2. Integrity in personal and organizational behaviors and practices (Autonomy)**

Nutrition and dietetics practitioners shall:

- a. Disclose any conflicts of interest, including any financial interests in products or services that are recommended. Refrain from accepting gifts or services which potentially influence, or which may give the appearance of influencing professional judgment.
- b. Comply with all applicable laws and regulations, including obtaining/maintaining a state license

- or certification if engaged in practice governed by nutrition and dietetics statutes.
- c. Maintain and appropriately use credentials.
- d. Respect intellectual property rights, including citation and recognition of the ideas and work of others, regardless of the medium (e.g. written, oral, electronic).
- e. Provide accurate and truthful information in all communications.
- f. Report inappropriate behavior or treatment of a patient/client by another nutrition and dietetics practitioner or other professionals.
- g. Document, code and bill to most accurately reflect the character and extent of delivered services.
- h. Respect patient/client's autonomy. Safeguard patient/client confidentiality according to current regulations and laws.
- i. Implement appropriate measures to protect personal health information using appropriate techniques (e.g., encryption).

### **3. Professionalism (Beneficence)**

Nutrition and dietetics practitioners shall:

- a. Participate in and contribute to decisions that affect the well-being of patients/clients.
- b. Respect the values, rights, knowledge, and skills of colleagues and other professionals.
- c. Demonstrate respect, constructive dialogue, civility and professionalism in all communications, including social media.
- d. Refrain from communicating false, fraudulent, deceptive, misleading, disparaging or unfair statements or claims.
- e. Uphold professional boundaries and refrain from romantic relationships with any patients/clients, surrogates, supervisees, or students.
- f. Refrain from verbal/physical/emotional/sexual harassment.
- g. Provide objective evaluations of performance for employees, coworkers, and students and candidates for employment, professional association memberships, awards, or scholarships, making all reasonable efforts to avoid bias in the professional evaluation of others.
- h. Communicate at an appropriate level to promote health literacy.
- i. Contribute to the advancement and competence of others, including colleagues, students, and the public.

### **4. Social responsibility for local, regional, national, global nutrition and well-being (Justice)**

Nutrition and dietetics practitioners shall:

- a. Collaborate with others to reduce health disparities and protect human rights.
- b. Promote fairness and objectivity with fair and equitable treatment.
- c. Contribute time and expertise to activities that promote respect, integrity, and competence of the profession.
- d. Promote the unique role of nutrition and dietetics practitioners.
- e. Engage in service that benefits the community and to enhance the public's trust in the profession.
- f. Seek leadership opportunities in professional, community, and service organizations to enhance health and nutritional status while protecting the public.

### **Glossary of Terms:**

**Autonomy:** ensures a patient, client, or professional has the capacity and self-determination to engage in individual decision-making specific to personal health or practice.<sup>1</sup>

**Beneficence:** encompasses taking positive steps to benefit others, which includes balancing benefit and risk.<sup>1</sup>

**Competence:** a principle of professional practice, identifying the ability of the provider to administer safe and reliable services on a consistent basis.<sup>2</sup>

**Conflict(s) of Interest(s):** defined as a personal or financial interest or a duty to another party which may prevent a person from acting in the best interests of the intended beneficiary, including simultaneous membership on boards with potentially conflicting interests related to the profession, members or the public.<sup>2</sup>

**Customer:** any client, patient, resident, participant, student, consumer, individual/person, group, population, or organization to which the nutrition and dietetics practitioner provides service.<sup>3</sup>

**Diversity:** “The Academy values and respects the diverse viewpoints and individual differences of all people. The Academy’s mission and vision are most effectively realized through the promotion of a diverse membership that reflects cultural, ethnic, gender, racial, religious, sexual orientation, socioeconomic, geographical, political, educational, experiential and philosophical characteristics of the public it services. The Academy actively identifies and offers opportunities to individuals with varied skills, talents, abilities, ideas, disabilities, backgrounds and practice expertise.”<sup>4</sup>



**Evidence-based Practice:** Evidence-based practice is an approach to health care wherein health practitioners use the best evidence possible, i.e., the most appropriate information available, to make decisions for individuals, groups and populations. Evidence-based practice values, enhances and builds on clinical expertise, knowledge of disease mechanisms, and pathophysiology. It involves complex and conscientious decision-making based not only on the available evidence but also on client characteristics, situations, and preferences. It recognizes that health care is individualized and ever changing and involves uncertainties and probabilities. Evidence-based practice incorporates successful strategies that improve client outcomes and are derived from various sources of evidence including research, national guidelines, policies, consensus statements, systematic analysis of clinical experience, quality improvement data, specialized knowledge and skills of experts.<sup>2</sup>

**Justice (social justice):** supports fair, equitable, and appropriate treatment for individuals<sup>1</sup> and fair allocation of resources.

**Non-Maleficence:** is the intent to not inflict harm.<sup>1</sup>

## References:

1. Fornari A. Approaches to ethical decision-making. *J Acad Nutr Diet.* 2015;115(1):119-121.
2. Academy of Nutrition and Dietetics Definition of Terms List. June, 2017 (Approved by Definition of Terms Workgroup Quality Management Committee May 16, 2017). Accessed October 11, 2017. <http://www.eatrightpro.org/~media/eatrightpro%20files/practice/scope%20standards%20of%20practice/academydefinitionoftermslist.ashx>
3. Academy of Nutrition and Dietetics: Revised 2017 Standards of Practice in Nutrition Care and Standards of Professional Performance for Registered Dietitian Nutritionists. *J Acad Nutr Diet.* 2018; 118: 132-140.
4. Academy of Nutrition and Dietetics “Diversity Philosophy Statement” (adopted by the House of Delegates and Board of Directors in 1995).

 <b>pennsylvania</b> DEPARTMENT OF HEALTH	<i>HR Bulletin</i> <b>Bureau of Human Resources</b>
<b>Subject:</b> Protected Health Information Confidentiality Policy	
<b>Date:</b> July 21, 2017	<b>Number:</b> 2017-06
By Direction of:    Daniel Ray Human Resources Director	References: <a href="#">Health Insurance Portability and Accountability Act of 1996 - HIPAA</a>

**Purpose:**

Department of Health (DOH) employees may come into contact with clients' protected health information during the course of everyday work. Federal and State laws (including the Health Insurance Portability and Accountability Act of 1996 – HIPAA) restrict the disclosure of protected health information except under certain circumstances. This policy sets forth general confidentiality standards applicable to the handling of protected health information with which all DOH employees must comply. Some offices will have specific policies that provide for additional or more stringent confidentiality standards, and these must be followed in addition to this policy.

**Definitions:**

**Confidential:** A status accorded to protected health information in the possession of the DOH indicating that it is subject to protection from disclosure and its dissemination is carefully controlled.

**Disclosure:** To communicate, transmit, or in any way convey any protected health information to any person or organization in any form.

**Facility:** Any institution or organization from which the DOH has obtained records that contain protected health information.

**Person:** A human being, living or deceased.

**Protected Health Information (PHI):** Information received, created, maintained, transmitted, or distributed that includes a person's past, present, or future physical or mental health condition; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that either: (1) identifies the individual; or (2) there is a reasonable basis to believe the information can be used to identify the individual. PHI can be either written or verbal information. PHI includes information such as an individuals' medical test results, medical histories, diagnoses, patient treatment regimens, etc. See Attachment A to this bulletin for a list of PHI Identifiers.

**Electronic Protected Health Information (ePHI):** PHI received, created, maintained, or distributed in electronic format.

**Policy:**

1. All PHI shall be treated as confidential at all times.
2. Each DOH employee may have access to PHI; therefore, it is the responsibility of each employee to protect the confidentiality of such information.
3. Paper documents, electronic files and other records containing PHI must be safeguarded to the greatest extent possible to avoid unauthorized disclosure.
4. Except in connection with their assigned responsibilities, employees are forbidden to access, discuss, or divulge PHI.
5. Employees are not authorized to respond to inquiries requesting PHI except through established DOH procedures.
6. Each employee must avoid unintentional disclosures of PHI.
7. Supervisors are responsible for ensuring their employees adhere to these standards and procedures.
8. Any breach of confidentiality must be immediately reported to the employee's supervisor. In addition to reporting the breach to appropriate supervisory personnel, as determined by each bureau, the breach must be reported to the DOH's Privacy Officer, Information Security Officer, and Chief Counsel's Office.
9. Employees must follow additional established DOH security policies and measures where applicable to safeguard PHI.
10. Any employee who has possession of, or access to PHI who willfully or negligently discloses such information to any person not entitled to receive it, or fails to properly secure the information, shall be subject to disciplinary action up to and including dismissal.

**Procedures:**

1. All records containing PHI, except when in use, are to be kept in secure electronic storage, file cabinets or in desks, out of sight of persons not authorized to have access to such information. At the end of the working day, all computers, desks or file cabinets containing such information are to be appropriately secured.
2. Documents containing PHI that are no longer needed or which have reached the end of their retention life per department/commonwealth policy, are to be shredded (not simply placed in wastebaskets). Where hard drives, portable USB flash drives, CD's, tapes, or any other electronic media are no longer needed for PHI storage, such media shall be wiped, cleaned, or destroyed according to Commonwealth standards.

3. Care is to be taken that PHI removed from DOH facilities is secured in a manner that will reduce the risk of theft or loss. Electronic data shall be secured via password and encryption controls, or other method explicitly authorized by the department's Information Security Officer.
4. Access to paper and electronic files containing PHI will be accessible only to those employees, who by virtue of their specific job assignment, have a need to utilize such information in the performance of their duties. Furthermore, access shall be restricted to the "minimum necessary" amount of information to do their job.
5. All ePHI's shall be encrypted and password protected. Passwords shall be kept confidential and are not to be shared. Additionally, passwords are not to be written where others might see or locate them. Keys to filing cabinets, desks or the like where PHI is stored are to be properly secured at all times.

**Responsibilities:**

**Employees:** All employees are required to read this PHI Confidentiality Policy, sign the attached acknowledgement form, Attachment B to this bulletin, and submit it to their bureau's administrative coordinator.

**Bureau Administrative Coordinators:** Bureau administrative coordinators must collect the signed acknowledgement forms, Attachment B, from all employees within their bureau and submit them to the Bureau of Human Resources, Labor Relations Section.

**Bureau of Human Resources:** HR staff will disseminate the PHI Confidentiality Policy to all DOH staff, receive the signed acknowledgement forms, Attachment B, from the bureau administrative coordinators, log receipt of each form into a tracking sheet, and file the forms into each employee's electronic Official Personnel File (eOPF). As new DOH staff are hired, HR staff will provide the PHI Confidentiality Policy to each new employee, have them sign and submit the acknowledgement form, record the submission into a tracking sheet, and file the form in the employee's eOPF. HR staff responsible for the hire of Temporary Clerical Pool employees will provide the PHI Confidentiality Policy to those employees, secure the signed acknowledgement form, and appropriately file the forms.

**Rescission:** HR Bulletin 2008-08, Personal Health Information Confidentiality Policy, Issue Date: December 9, 2008.

Questions should be directed to the Bureau of Human Resources, Labor Relations section at (717) 547-3184.

ATTACHMENT A

**List of Protected Health Information Identifiers**

1. Names
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death.
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers.
13. Device identifiers and serial numbers.
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints.
17. Full face photographic images and any comparable images.
18. Any other unique identifying number, characteristic, or code.

Source: Mathematica Policy Research Report, Minimizing Disclosure Risk in HHS Open Data Initiatives, September 29, 2014, [https://aspe.hhs.gov/system/files/pdf/77196/rpt\\_Disclosure.pdf](https://aspe.hhs.gov/system/files/pdf/77196/rpt_Disclosure.pdf)





ACKNOWLEDGMENT OF RECEIPT  
PROTECTED HEALTH INFORMATION CONFIDENTIALITY POLICY

I acknowledge that I have reviewed the Pennsylvania Department of Health's Protected Health Information Confidentiality Policy.

Employee Name (print): \_\_\_\_\_

Employee Personnel Number: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Bureau: \_\_\_\_\_

**RELEASE FROM LIABILITY**

I, \_\_\_\_\_, volunteer, will be participating in a Dietetic Internship with the Department of Health. I agree to the following:

1. My participation as an Intern does not give me the status of an employee or agent of the Pennsylvania Department of Health or the Commonwealth of Pennsylvania.
2. By signing this document, I agree to release the Commonwealth of Pennsylvania from any liability arising from my activities and work as a volunteer. This release also applies to my heirs, executors, or administrators who could bring a legal action in my place. By releasing the Commonwealth from liability, I also release its agents and employees from liability. This release covers all causes of action, lawsuits, awards for damages, judgments, claims, or demands which arise from my activities and participation as a volunteer.

\_\_\_\_\_  
Witness Signature


\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Date

# MANAGEMENT DIRECTIVE

## Commonwealth of Pennsylvania Governor's Office

<b>Subject:</b> Commonwealth of Pennsylvania Information Technology Acceptable Use Policy	<b>Number:</b> 205.34 Amended
<b>Date:</b>  January 22, 2016	<b>By Direction of:</b>  Sharon P. Minnich, Secretary of Administration
<b>Contact Agency:</b> Office of Administration, Office for Information Technology, Telephone 717.787.5440 Email <a href="mailto:ra-ITCentral@pa.gov">ra-ITCentral@pa.gov</a>	

**This directive establishes policy, responsibilities, and procedures for the acceptable use of Information Technology (IT) resources by Authorized Users. Marginal dots are excluded due to major changes.**

- 1. PURPOSE.** To establish policy, responsibilities, and procedures to provide Authorized Users with guidelines for, restrictions upon, and standards for the acceptable use of IT Resources. Covered IT Resources include those that are connected from any location to the commonwealth's computer systems including the Metropolitan Area Network (MAN), which is the commonwealth's computer network that spans the state and provides connectivity for Local Area Networks (LANs), as well as the internet; and IT Resources that are not connected to or used in conjunction with the MAN.
- 2. SCOPE.** This directive applies to all Authorized Users of all departments, boards, commissions, and councils (hereinafter referred to as "agencies") under the Governor's jurisdiction and contractors, consultants, volunteers, and any other Authorized User who utilizes or has access to IT Resources.
- 3. OBJECTIVE.** To ensure that all Authorized Users that have access to IT Resources are made aware of and comply with the standards and policy set forth in this directive and in Enclosure 1, Commonwealth Acceptable Use Standards for Information Technology (IT) Resources.
- 4. DEFINITIONS.**
  - a. Authorized Users.** Commonwealth of Pennsylvania employees, contractors, consultants, volunteers or any other user who utilizes or has access to IT Resources.
  - b. Electronic Communication System.** Any method of electronic communication or information system that generates, stores, transmits, or displays information, including, but not limited to:

- (1) The commonwealth's Metropolitan Area Network;
- (2) Local Area Networks;
- (3) The Internet;
- (4) News groups;
- (5) Bulletin board systems;
- (6) Intranets;
- (7) Social media;
- (8) Blogs;
- (9) Computer hardware;
- (10) Software programs;
- (11) Applications;
- (12) Voice mail systems;
- (13) Telephones;
- (14) Faxes;
- (15) Radio;
- (16) Cellular and smartphones;
- (17) Electronic mail and messaging systems;
- (18) Instant Messaging;
- (19) Text Messaging;
- (20) Cloud storage solutions;
- (21) Video conferencing and transmissions; and
- (22) Electromagnetic, photo-electronic, and other electronic media or devices.

**c. IT Resource.** Any commonwealth computer system, Electronic Communication System, or electronic resource used for electronic storage and/or communications, including, but not limited to:

- (1) Servers;
- (2) Laptops;
- (3) Desktop computers;
- (4) Copiers;
- (5) Printers;
- (6) Wired or wireless telephones;
- (7) Cellular phones or smartphones;
- (8) Tablets;
- (9) Wearables;
- (10) Pagers;
- (11) All other mobile devices; and
- (12) Commonwealth contractor-provided IT Resources of all kinds.

## 5. POLICY.

- a. **Authorized Users of IT Resources are required to understand and abide by this directive and the Acceptable Use Standards.** These Acceptable Use Standards are designed to prevent use that may be illegal, unlawful, abusive, or which may have an adverse impact on the commonwealth or its IT Resources. In addition, they identify for Authorized Users the permissible and effective uses of IT Resources. Authorized Users are encouraged to assist in the enforcement of these Acceptable Use Standards by promptly reporting any observed violations to their supervisor, the human resources office, agency contact or contracting officer. Enclosure 1, Commonwealth Acceptable Use Standards for Information Technology (IT) Resources, sets forth additional information about the permissible scope of usage of IT Resources.
- b. **Abuse or misuse of IT Resources will have consequences.** The improper use of commonwealth IT Resources by employees or volunteers may result in disciplinary action, up to and including termination of employment or volunteer status, depending on the circumstances of the incident. The improper use of IT Resources by contractors or consultants may result in disciplinary action that may include termination of engagement, and other formal action under the terms of the applicable contract or debarment under the Contractor Responsibility Program set forth in [Management Directive 215.9, Contractor Responsibility Program](#). When warranted, the commonwealth or its agencies may pursue or refer matters to other appropriate authorities for investigation regarding potential violation of local, state, or federal laws through the misuse of IT Resources.
- c. **Ownership of IT Resources.** All data and records, including those pertaining to computer use, Internet use, email communication, voicemail communication, text messages, and other electronic communication (whether sent, received, or stored), as well as the content of such communications, are

presumed to be the sole and exclusive property of the commonwealth. Individual Authorized Users do not control the access to or the use of such data or records. In addition, Authorized Users have no property or other rights to any or all related physical equipment, hardware, and software applications that are provided, stored, or otherwise utilized in connection with IT Resources.

- d. Authorized Users should have no expectation of privacy when using IT Resources.** At its discretion, executive level or human resources staff or their authorized designees may access IT Resources in any way, including to retrieve, search, trace, audit, monitor and review any files, data, or records which are stored on or accessed through IT Resources, as well as, data or records related to IT Resource usage, including Internet records or email communications, for business purposes, or in order to determine compliance with the provisions of this directive or any other directive, personnel policy or applicable local, state, or federal law. Agency heads may determine who may access these files, data, and records, including, but not limited to, executive level staff, legal staff, human resource management staff, network or security system administrators, individuals in the Authorized User's chain of command or others, including law enforcement. Files, data, and records which are stored on IT Resources together with records of IT Resources use may be reviewed at any time and are routinely backed up and stored without the user's knowledge. As such, Authorized Users should have no expectation of privacy in any electronic files, data, or records stored on or accessed through IT Resources nor should an Authorized User have any expectation of privacy in any communications sent or received via, or stored within, IT Resources.
- e. IT Resources are subject to monitoring or other access by authorized commonwealth personnel.** All IT Resources and files, data, or records stored on or accessed through IT Resources may be accessed in any way (including but not limited to being traced, audited, monitored, reviewed, logged, blocked, searched, retrieved, or recorded) by authorized commonwealth personnel with or without notice to the Authorized User.
- f. Use of an IT Resource by an Authorized User is deemed to be consent to all access by authorized commonwealth personnel.** By using an IT Resource, Authorized Users consent to all access by authorized commonwealth personnel, including but not limited to use being traced, audited, monitored, reviewed, logged, blocked, searched, retrieved, or recorded, with or without notice.
- g. Authorized Users may not access unauthorized data and should take measures to protect the security of their data.** As part of the privilege of being an Authorized User, Authorized Users may not attempt to access any data or programs contained on commonwealth systems for which they do not have authorization or explicit consent. Authorized Users must use passwords and/or encryption in a manner that is consistent with commonwealth policy. Utilization of special passwords or encryption does not, however, guarantee the confidentiality of any electronic communication or of any file, data, or record stored or accessed through IT Resources. Authorized Users must keep passwords secure and must not share them with others.
- h. IT Resources are intended for business use and should be used primarily for that purpose.** IT Resources are tools that the commonwealth has made available for commonwealth business purposes. Where personal use of IT Resources does not interfere with the efficiency of operations and is not otherwise in conflict with the interests of the commonwealth, reasonable use for personal purposes will be permitted in accordance with standards established for business use. Such personal use shall be limited, occasional, and incidental. Any personal use which is inconsistent with commonwealth policy regarding availability or capability of IT Resources, or inappropriate content of communications as defined by this policy is prohibited.

- i. **IT Resources must never be used in a manner that violates other commonwealth directives and policies.** All use of IT Resources must conform with [Executive Order 1980-18, Code of Conduct, Management Directive 505.7, Personnel Rules](#), and commonwealth policies on nondiscrimination and prohibition of sexual harassment. Violations of these issuances and policies through IT Resources will be treated in the same manner as other violations.
- j. **All Authorized Users must be provided with this directive.** All current commonwealth employees must be provided a copy of this policy. All new employees must review this policy during new employee orientation. All non- commonwealth employee Authorized Users must review this policy prior to their use of and access to commonwealth IT Resources. Copies may be provided either electronically or in hard copy.
- k. **All Authorized Users must sign an Acknowledgement of Receipt Form.** On an annual basis agencies must obtain signed user agreements from Authorized Users **prior** to granting access to IT Resources. Employees or volunteers shall sign Enclosure 2 to this directive, Commonwealth IT Resources Acceptable Use Policy User Agreement Commonwealth Employee or Volunteer Form. Contractors and consultants shall sign Enclosure 3 to this directive, Commonwealth IT Resources Acceptable Use Policy User Agreement Commonwealth Contractor or Consultant Form.
- l. **Each agency must maintain copies of the agreement signed by each Authorized User in that agency.** Completed user agreements shall be maintained as part of the employee's Official Personnel Folder. Alternately, Authorized Users may sign and agencies may store these agreements in an electronic format consistent with [Management Directive 210.12, Electronic Commerce Initiatives and Security](#), and [ITP-SEC006, Commonwealth of Pennsylvania Electronic Signature Policy](#). Signed agreements must be accessible to individuals who are authorized to view or use the documents.
- m. **Requests for electronic records should be treated in the same manner as paper records.** Requests for records pertaining to IT Resources must be addressed consistent with all laws, directives, or policies that would apply to the same information if maintained in a non-electronic format. These requests should be referred to agency legal counsel and/or the Agency Open Records Officer, as appropriate.
- n. **This amended directive supersedes prior or inconsistent policies.** This policy supersedes any existing IT, Internet and/or email use policy issued by agencies under the Governor's jurisdiction that is inconsistent with this directive, unless specific exemptions are granted by the Secretary of Administration or designee. Approved labor agreements, side letters or current practices should be applied in a manner to effectuate both this policy and any such agreement, side letter or current practice. In cases where a provision of an approved labor agreement, side letter or current practice cannot be reconciled with this policy, the former shall control. Agencies may develop supplemental IT, Internet and/or email use policies only with the approval of the Secretary of Administration or designee.

## 6. RESPONSIBILITIES.

### a. Agency shall:

- (1) Provide either a hard copy or electronic copy of this directive to Authorized Users.

- (2) Ensure that Authorized Users have signed the user agreement.
- (3) Maintain a copy of the signed user agreement for Authorized Users.

**b. Authorized Users** shall:

- (1) Understand the permissible scope of usage of IT Resources.
- (2) Sign the user agreement.

**c. Enterprise Information Security Office** may:

- (1) Conduct system audits and compliance reviews of adherence to this directive.
- (2) Prevent and respond to cyber security incidents.
- (3) Assist human resources staff in conducting investigations involving the alleged misuse of IT Resources.
- (4) Assist in data retrieval and analysis for any records requests.

**7. RELATED GUIDANCE/REFERENCES.** Additional technical standards for IT Resources usage will be published in the Office of Administration, Office for Information Technology (OA/OIT), [Information Technology Policies](#) are available on the OA/OIT website.

**Enclosure 1 - Commonwealth Acceptable Use Standards for Information Technology (IT) Resources**

**Enclosure 2 – Commonwealth IT Resources Acceptable Use Policy User Agreement Commonwealth Employee or Volunteer Form**

**Enclosure 3 – Commonwealth IT Resources Acceptable Use Policy User Agreement Commonwealth Contractor or Consultant Form**

**This directive replaces in entirety, *Management Directive 205.34*, dated November 17, 2011.**



# COMMONWEALTH ACCEPTABLE USE STANDARDS FOR

## INFORMATION TECHNOLOGY (IT) RESOURCES

Each Authorized User must comply with [\*Management Directive 205.34, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy\*](#) and the following Acceptable Use Standards when using IT Resources:

### **AUDITING, MONITORING AND REPORTING**

All IT Resources and files, data, or records stored on or accessed through IT Resources may be accessed in any way (including but not limited to being traced, audited, monitored, reviewed, logged, blocked, searched, retrieved, or recorded) by authorized commonwealth personnel with or without notice to the Authorized User.

Authorized Users, therefore, should have no expectation of privacy in any files, data or records stored on or accessed through IT Resources, nor should they have any expectation of privacy in any electronic communication sent or received via, or stored within, IT Resources. By using IT Resources, the user authorizes any access to IT Resources by the commonwealth.

Authorized Users are encouraged to assist in the enforcement of these Acceptable Use Standards by promptly reporting any observed violations to their supervisor, the human resources office, agency contact or contracting officer.

### **DISCIPLINE OR OTHER CONSEQUENCES OF MISUSE**

The improper use of IT Resources by employees or volunteers may result in disciplinary action, up to and including termination of employment or volunteer status, depending on the circumstances of the incident. The improper use of IT Resources by contractors or consultants may result in disciplinary action that may include termination of engagement, other formal action under the terms of the applicable contract, or suspension or debarment under the Contractor Responsibility Program. When warranted, the commonwealth or its agencies may pursue or refer matters to other appropriate authorities for investigation regarding potential violation of local, state, or federal laws through the misuse of IT Resources.

### **GENERAL IT RESOURCES USE**

As part of the privilege of being an Authorized User, Authorized Users may not attempt to access any data or programs contained on commonwealth systems for which they do not have authorization or explicit consent.

- a.** Authorized Users are strictly responsible for maintaining the confidentiality of their commonwealth or agency account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes (such as multi-factor authentication methods).
- b.** Authorized Users may not make unauthorized copies of software.
- c.** Authorized Users may not use non-standard shareware or freeware software without agency IT management approval.
- d.** Authorized Users may not purposely engage in activity that may: harass, threaten, or abuse others; degrade the performance of IT Resources; deprive an Authorized User of access to an IT Resource; obtain extra IT Resources beyond those allocated; or circumvent IT Resource security measures.
- e.** Authorized Users may not use IT Resources to engage in personal, for-profit transactions or business, or to conduct any fundraising activity not specifically sponsored, endorsed, or approved by the commonwealth.
- f.** Authorized Users may not engage in illegal activity in connection with their use of IT Resources, including, but not limited to downloading, installing, and/or running security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, Authorized Users may not run password cracking programs, packet sniffers, port scanners, or any other non-approved programs on IT Resources, unless they are authorized to do so.
- g.** Authorized Users may not access, create, store, transmit, post, or view material that is generally considered to be inappropriate or personally offensive or which may be construed as discriminatory or harassing, including sexually suggestive, pornographic, or obscene material.
- h.** Authorized Users are personally responsible for the security of authorized portable and mobile IT Resources and devices. Care must be exercised to ensure these devices are secured and not lost, stolen or otherwise accessed in an unauthorized manner.
- i.** Authorized Users may not store non-public information on IT Resources, if those IT Resources may be removed from commonwealth facilities without prior approval from the agency Secretary or designee.
- j.** Authorized Users shall use commonwealth approved electronic communication systems primarily for commonwealth business.
- k.** Authorized Users shall use only commonwealth approved encryption methods to encrypt information, as appropriate.
- l.** Authorized Users shall use only commonwealth approved storage devices or storage solutions.
- m.** Authorized Users may only store or transmit commonwealth content, files, data or any other type of information on or through an IT Resource that is commonwealth-provided or commonwealth-approved..

## **INTERNET USE**

All security policies of the commonwealth and its agencies, as well as policies of Internet websites being accessed, must be strictly adhered to by Authorized Users.

## **Software**

In connection with Authorized Users' use of and access to IT Resources:

- a.** All software used to access IT Resources must be part of the agency's standard software suite or approved by the agency IT department. This software must incorporate all vendor provided security patches.
- b.** All files downloaded from the Internet must be scanned for viruses using the approved commonwealth distributed software suite and current virus detection software.
- c.** All software used to access the Internet shall be configured to use an instance of the commonwealth's standard Internet Access Control and Content Filtering solution.

## **Access Control and Authorization**

Agencies should authorize access to the Internet using commonwealth IT Resources through the utilization of a user ID/password system. Security violations can occur through unauthorized access, and all possible precautions should be taken to protect passwords. Authorized Users are responsible for activity and communications, including but not limited to email, voicemail, text messages, data, and any other electronic communications transmitted under their account.

## **Incidental Use**

- a.** IT Resources are communication tools that the commonwealth has made available for commonwealth business purposes. Where personal use of these resources does not interfere with the efficiency of operations and is not otherwise in conflict with the interests of the commonwealth, reasonable use for personal purposes will be permitted in accordance with standards established for business use. Such personal use shall be limited, occasional, and incidental.
- b.** Incidental personal use of Internet access is restricted to Authorized Users; it does not extend to family members, other acquaintances, or any other persons.
- c.** Access to IT Resources that are home-based, e.g., accessing the Internet from an agency owned, home-based computer, must adhere to all the same policies that apply to use from within agency facilities.
- d.** Employees may not allow family members or other non-employees to access commonwealth provided home-based IT Resources.
- e.** Incidental use must not result in direct costs to the commonwealth.
- f.** Incidental use must not interfere with the normal performance of an Authorized User's work duties.

- g.** Incidental use may not risk legal liability for, or embarrassment to, the commonwealth.
- h.** All files and documents located on IT Resources, including personal files and documents may be accessed and retrieved in accordance with this policy. In addition, it should be understood that such documents may be subject to disclosure under the *Right-to-Know Law, 65 P.S. §§ 67.101–67.3104*, and other laws.

### **Acceptable Use of the Internet**

Accepted and encouraged use of the Internet for Authorized Users on IT Resources includes, but is not limited to, the following:

- a.** Access, research, exchange, or posting of information that relates to the assigned job duties of an Authorized User for carrying out commonwealth business.
- b.** Promotion of public awareness in regard to commonwealth law, agency services, and public policies.
- c.** Posting of agency information that has been authorized by appropriate management.

### **Acceptable use of Instant Messaging (IM)**

- a.** Only Authorized Users who have been granted agency level approval to utilize IM technology may use IM software, and they may use it only to communicate internally across the commonwealth MAN in a manner directly related to an Authorized User's job responsibilities.
- b.** IM software that is utilized by commonwealth Authorized Users must be part of the determined enterprise standard software solution.
- c.** IM software is only to be used to conduct state business that produces records that have little or no documentary or evidentiary value and that need not be set aside for future use. These records are subject to the provisions of [Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program](#) and [Manual 210.9, The Commonwealth's General Records Retention and Disposition Schedule](#), items G001.021, Transitory Records and G001.025, Transitory Files Confidential.

### **Acceptable use of Social Media**

- a.** Social Media may include, but are not limited to, blogs, RSS, discussion boards, social networking, wikis, video sharing sites, mashups, and social tagging.
- b.** Only Authorized Users who have been granted agency level approval to do so may utilize Social Media, and only if the use is directly related to an Authorized User's job responsibilities. Please refer to [Management Directive 205.42, Social Media](#).
- c.** Social Media may be used only to conduct commonwealth business that produces records that have little or no documentary or evidentiary value and that need not be set aside for future use. These

records are subject to the provisions of [Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program](#) and [Manual 210.9, The Commonwealth's General Records Retention and Disposition Schedule](#), items G001.021, Transitory Records and G001.025, Transitory Files Confidential.

### **Acceptable Use of Mobile Technologies**

Authorized Users shall ensure that information on mobile devices is not compromised by:

- a.** Securing mobile devices from access by unauthorized persons, through the use of locking devices, passwords, or other appropriate protection;
- b.** Ensuring that unauthorized persons do not view information on the display screen;
- c.** Refraining from checking devices into airline luggage systems, with hotel porters, or from using other unsupervised handling or storage processes;
- d.** Securing or maintaining possession of mobile devices at all times; and
- e.** Immediately reporting a lost or stolen mobile device to their supervisor.

### **Acceptable Use of Cloud Storage Solutions**

- a.** Cloud storage solutions enable convenient, on-demand network access to a shared pool of configurable computing resources such as storage that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud storage solutions are intended for business use and shall be used primarily for that purpose.
- b.** Cloud storage solutions must never be used in a manner that violates other commonwealth directives and policies. The use of cloud storage solutions must conform with [Executive Order 1980-18, Code of Conduct](#), [Management Directive 505.7, Personnel Rules](#), and the [Management Directive 205.34 Amended, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy](#). Violations of these issuances and policies through IT Resources will be treated in the same manner as other violations.
- c.** All files and documents located in cloud storage solutions are generally owned by the commonwealth and may be accessed and retrieved in accordance with this policy. In addition, it should be understood that such documents may be subject to requests for disclosure under the *Right to Know Law, 65 P.S. §§ 67.101—67.3103*, and other similar laws.
- d.** Users will only access those cloud storage solutions which have been authorized for their use.
- e.** Users who obtain a password and ID for a cloud storage solution shall keep that password confidential. Commonwealth policy prohibits the sharing of user IDs or passwords obtained for access to network and cloud storage resources.
- f.** Users are responsible for the use of their individual cloud storage accounts and should take all reasonable precautions to prevent others from being able to use their account, including coworkers, friends, or family.

- g.** Any user placing sensitive data into Cloud Storage Solutions must (in concert with his or her chain of command and/or Chief Counsel's Office, as appropriate) evaluate the risk to the data's security, privacy, and availability. No commonwealth policy or procedure may be violated via use of a Cloud Storage Solution unless that policy or procedure is itself explicitly waived.

### **EMAIL USE Usage**

- a.** When sensitive material is sent electronically via email, it is important to verify that all recipients are authorized to receive such information and to understand that email is not fully secure and/or private, except where appropriate security applications are used, e.g. data encryption.
- b.** Users should understand that messages can be quickly and easily copied and may be forwarded inappropriately.
- c.** Where it is necessary to transmit commonwealth proprietary or restricted information beyond the commonwealth email network, the messages should be protected by encryption. Authorized Users should contact their agency Network Coordinator or IT Coordinator for assistance if encryption is needed.
- d.** Email messages to be transmitted outside of the United States should comply with local laws governing international transmission of data as well as United States export control regulations. For assistance, Authorized Users should contact their Network Coordinator or IT Coordinator, who may receive technical assistance from the Office of Administration, Office for Information Technology (OA/OIT).
- e.** The agency head or designee should determine specific agency policy regarding business information which is determined to be too confidential or sensitive to be transmitted via email.
- f.** All user activity and electronic communication, including the contents of such communication, including but not limited to, email, voicemail, text messages and data, on IT Resources is subject to access, including tracking, blocking, logging, auditing, monitoring, retrieving, and reviewing as described more fully in this directive.
- g.** Authorized Users shall use email addresses assigned to them primarily for work-related purposes. Authorized Users may not use their commonwealth e-mail address to register or subscribe for any product or service that is not work-related.
- h.** Authorized Users shall not forward work related emails, calendar items or documents to their personal non-commonwealth email addresses. In the event that a provision of an approved labor agreement, side letter or current practice cannot be reconciled with this policy, the former will control.

### **Access Control and Authorization**

- a.** Only Authorized Users may use IT Resources to send or view email or access the commonwealth's email systems.

- b.** Only after agreement to abide by all applicable rules of the system, including this directive and its related Acceptable Use Standards, shall access to commonwealth email be granted to commonwealth employees, contractors, consultants, and volunteers, in their capacity as Authorized Users.
  
- c.** An Authorized User may not access the email or account of another Authorized User. This restriction does not apply to system administrators and management staff in the Authorized User's chain of command authorized to access email for legitimate business purposes, to effectuate [Management Directive 205.34, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy.](#)
  
- d.** In accordance with agency policy, Authorized Users shall use password protection to limit access to email files. Authorized Users shall safeguard their passwords so that unauthorized users do not have access to their email. Authorized Users are responsible for all messages transmitted and originating under their account.

### **Message Retention**

All messages, including email, text messages, and voicemail messages are subject to the appropriate records retention and disposition schedules and the provisions of [Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program.](#)

### **Email Security Issues, Worms, and Viruses**

Email and attachments to email are sources of computer security issues. All Authorized Users should act in accordance with the latest IT Policies regarding containment methods for computer viruses and any security alert emails from agency HR or IT.

### **Maintaining Professionalism**

Every Authorized User who uses IT Resources is responsible for ensuring posted messages and other electronic communications are professional and businesslike. As a way to impose personal restraint and professionalism, all Authorized Users should assume that whatever they write may at some time be made public. Authorized Users should follow the following guidelines:

- Be courteous and remember that you are representing the commonwealth with each email message sent.
  
- Review each email message before it is sent and make certain that addresses are correct and appropriate. Use spell check before sending.
  
- Consider that each email message sent, received, deleted, or stored has the potential to be retrieved, seen, and reviewed by audiences, including the general public, who were not the intended recipients of the message.

- Ensure that content is appropriate and consistent with business communication; avoid sarcasm, exaggeration, and speculation which could be misconstrued. Remember that intonation and inflection are lost in email.
- Be as clear and concise as possible; be sure to clearly fill in the subject field so that recipients of email can easily identify different email messages.

### **Electronic Message Distribution, Size, and Technical Standards**

- a. Authorized Users should receive authorization from their supervisors before wide scale “broadcasting” an email bulletin to groups of employees.
- b. The use of “reply to all” should be avoided unless it is appropriate to respond to all addressees.
- c. Authorized Users wishing to send email bulletins to all commonwealth or agency employees must first obtain authorization from agency management.
- d. Email messages should be brief, and attachments to email messages should not be overly large. Agency IT staff will inform Authorized Users of limitations on the size of email messages and attachments. OA/OIT periodically will provide technical standards and guidance to agencies through IT Policies on the technical capacities of the commonwealth email system and limitations on email message size. Technical standards will be provided in areas such as file size and backup procedures, and will be available on the OA/OIT website at <http://www.oit.state.pa.us>.

### **UNACCEPTABLE USES OF IT RESOURCES**

The following are examples of impermissible uses of IT Resources. This list is by way of example and is not intended to be exhaustive or exclusive. Authorized Users are prohibited from:

- Accessing, creating, storing, transmitting, posting, or viewing material that is generally considered to be inappropriate or personally offensive or which may be construed as harassing, including sexually suggestive, pornographic, or obscene material.
- Accessing, creating, storing, transmitting, posting, or viewing material that expresses or promotes discriminatory attitudes toward race, gender, age, nationality, religion, or other groups including, but not limited to, protected groups identified in [Executive Order 2003-10, Equal Employment Opportunity](#).
- Engaging in personal, for-profit transactions or business, or conducting any fundraising activity not specifically sponsored, endorsed, or approved by the commonwealth.
- Participating in Internet activities that inhibit an employee’s job performance or present a negative image to the public, such as auctions, games, or any other activity that is prohibited by directive, policy, or law.
- Attempting to test or bypass the security (“hacking” or “cracking”) of IT Resources or to alter internal or external IT Resource security systems.



- Participating in or promoting computer sabotage through the intentional introduction of computer viruses, worms, or other forms of malware, i.e. malicious software.
- Promoting, soliciting, or participating in any activities that are prohibited by local, state, or federal law or the commonwealth rules of conduct.
- Violating or infringing the rights of any other person.
- Using any other Authorized User's password and/or equipment to conduct unacceptable activities on IT Resources.
- Harassing or threatening activities including, but not limited to, the distribution or solicitation of defamatory, fraudulent, intimidating, abusive, or offensive material.
- Transmitting or soliciting any proprietary material, such as copyrighted software, publications, audio, or video files, as well as trademarks or service marks without the owner's permission.
- Promoting or participating in any unethical behavior or activities that would bring discredit on the commonwealth or its agencies.
- Downloading and/or installing any unapproved software.
- Transmitting or posting any messages that intentionally misrepresent the identity of the sender, hide the identity of the sender, or alter a sender's message.
- Sending or forwarding commonwealth information or records through noncommonwealth email or webmail accounts. Examples of non-commonwealth email accounts include, but are not limited to, Hotmail, Yahoo mail, Gmail, or email provided by other Internet service providers.
- Sending, forwarding, or storing commonwealth information or records utilizing noncommonwealth accredited mobile devices. Examples of mobile devices include, but are not limited to:
  - tablets, smart phones, pagers, wearables, and cellular telephones.
- Participating in any other Internet or email use that is deemed inappropriate by the commonwealth and/or its agencies and is communicated as such to Authorized Users.
- Using or disclosing confidential material covered by law or commonwealth policy.

# COMMONWEALTH IT RESOURCE ACCEPTABLE USE POLICY USER AGREEMENT –

## COMMONWEALTH EMPLOYEE/INTERN

This user agreement does not prohibit employees/Interns from performing authorized job duties.

I have read the attached *Management Directive 205.34, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*, and Enclosure 1, Commonwealth Acceptable Use Standards for Information Technology, and in consideration of the Commonwealth of Pennsylvania making its IT Resources available to me, I agree to abide by the requirements set forth therein. I understand that disciplinary action, up to and including termination, may be taken if I fail to abide by any of the requirements of this directive.

I further understand that my commonwealth IT Resource usage, including electronic communications such as email, voicemail, text messages, and other data and records, may be accessed and monitored at any time, with or without advance notice to me. By signing this agreement, I specifically acknowledge and consent to such access and monitoring.

I further understand that if I have any questions regarding this directive, I am required to ask for clarification from the PA WIC DI Program Director or PA WIC agency human resource representative.

Printed Name: \_\_\_\_\_

Employee Number: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Agency: \_\_\_\_\_

Bureau/Facility: \_\_\_\_\_

Division/Section: \_\_\_\_\_

Mailing Address: \_\_\_\_\_

Email Address: \_\_\_\_\_

Work Phone: \_\_\_\_\_

Optional Agency Approval: \_\_\_\_\_

Date: \_\_\_\_\_



**PA WIC Dietetic Internship Program**

**Intern Handbook Acknowledgement Form**

I acknowledge that I am responsible for knowing, understanding, and abiding by the policies and procedures governing the PA WIC Dietetic Internship program. I understand that failure to follow any of the policies and procedures will result in disciplinary action.

Printed Name: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

---

**PA WIC Dietetic Internship Program**

**Academy of Nutrition and Dietetics**

**Code of Ethics Acknowledgement Form**

I, \_\_\_\_\_, am a Dietetic Intern in the PA WIC Dietetic Internship Program. I have read the Code of Ethics for the Profession of Dietetics. I understand its guidelines, and I agree to uphold its ethical principles. As a student member of the Academy of Nutrition and Dietetics and as a future ACEND-credentialed dietetics practitioner, I agree to abide by the Code. I understand that failure to follow the Code of Ethics will result in disciplinary action.

Printed Name: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_