



UNITED STATES DEPARTMENT OF EDUCATION

WASHINGTON, DC 20202

April 10, 2017

Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight
and Government Reform
United States House of Representatives
Washington, DC 20515

Dear Congressman Cummings:

Thank you for your letter to Secretary DeVos regarding the U.S. Department of Education's (Department's or ED's) implementation of the Federal Records Act (FRA) and the Freedom of Information Act (FOIA). I am pleased to respond on behalf of the Secretary. I am also sending an identical response to Chairman Chaffetz.

The Department has a robust records management program located within the Office of Management (OM). We are proud of the quality of our records management program, and of the fact that we scored 93 (of a possible 100) on the National Archives and Records Administration's (NARA's) 2016 records management self-assessment, as well as scoring 3.5 (out of a possible 4.0) for our email management capability maturity model. Transparency and preserving official records are core values here at the Department, and I am happy to respond to your six requests as follows:

Request 1

From January 1, 2016, to January 19, 2017, the Secretary, Deputy Secretary, and Under Secretary used alias accounts to manage the large volume of email received (e.g., the Deputy Secretary used "deputysecretary@ed.gov"). Currently, the Department only has one alias email account, and it is used by the Secretary.

Requests 2-4

In response to your requests 2, 3, and 4, I am enclosing four policies regarding records management and social media. The Department records management policies are described in the attached Department directive OM:6-103, "Records and Information Management Program." Section II of this directive incorporates the electronic messaging requirements of the Presidential and Federal Records Act Amendments of 2014. As noted in this directive, the Department prohibits the use of non-official email accounts to conduct official government business. This policy also strongly discourages the use of non-email electronic messaging technologies (such as instant mail and text messaging) when creating communications that may be Federal records. Nevertheless, this directive clarifies that Federal records created while using these technologies must be forwarded to the Department email system within 20 days for recordkeeping purposes.

www.ed.gov

The Department of Education's mission is to promote student achievement and preparation for global competitiveness by fostering educational excellence and ensuring equal access.

The specific email encryption applications referenced in your letter (Signal, Confide, and WhatsApp) are not approved for use within the Department network.

The Department's social media policies are contained in Departmental directive OCIO:3-109, "ED Social Media Policy," that states "[a]ll social media content is subject to the Federal Records Act and National Archives and Records Administration (NARA) and ED records schedules and related requirements." The sponsors of web content are responsible for compliance with the related records management requirements. I am also enclosing two additional guidance documents related to social media records management, Joint Guidance on Instant Messaging and Text Messaging Pilot Program and Web 2.0 and Social Media Records Management Guidance, June 2011.

Request 5

In response to request number 5 regarding our agency's FOIA policy, individuals are required to search for potentially responsive materials in all possible formats and locations, including non-official email accounts, texts, IMs, and social media communications.

Request 6

I am pleased to report that the Department is in compliance with the Office and Management Budget Memorandum, M-12-18, the Managing Government Records Directive, issued on August 24, 2012, and (subject to available appropriations) that we expect to meet the 2019 deadline for managing permanent records in electronic format.

I appreciate the opportunity to respond to your letter and hope this information is helpful. If you have further questions or need additional information, please have your staff contact Molly Petersen, Acting Assistant Secretary, Office of Legislation and Congressional Affairs, at (202) 401-0020.

Sincerely,

A handwritten signature in blue ink, appearing to read "Kathleen M. Styles", with a stylized flourish extending to the right.

Kathleen M. Styles
Chief Privacy Officer

Enclosures:

1. Departmental directive OM:6-103, "Records and Information Management Program"
2. Departmental directive OCIO-3:109, "ED Social Media Policy"
3. Joint Guidance on Instant Messaging and Text Messaging Pilot Program
4. Web 2.0 and Social Media Records Management Guidance, June 2011

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
MINORITY (202) 225-6051
<http://oversight.house.gov>

March 8, 2017

The Honorable Betsy Devos
Secretary
Department of Education
400 Maryland Avenue, S.W.
Washington, D.C. 20202

Dear Madam Secretary:

Federal recordkeeping and government transparency laws such as the Federal Records Act and the Freedom of Information Act (FOIA) ensure the official business of the government is properly preserved and accessible to the American public.¹ As the Committee with legislative jurisdiction over these laws, we have a longstanding interest in ensuring compliance with their provisions.² Over the past decade, our oversight has included monitoring trends in federal employees' use of technology in order to ensure the statutory requirements of these laws keeps pace with their original purpose. The Committee has authored several updates to these laws, such as the Presidential and Federal Records Act Amendments of 2014 and the FOIA Improvement Act of 2016.³ We plan to pursue additional efforts to update these laws.

Federal Records Act challenges have spanned across administrations. A 2013 report by the Inspector General for the Commodities Futures Trading Commission found that former Chairman Gary Gensler used his personal email consistently.⁴ Documents produced as part of the Committee's investigation into the Department of Energy's disbursement of funds under the Recovery Act showed that the former Executive Director of the Loan Program Office Jonathan Silver often used his personal email account to conduct official business.⁵

¹ Pub. L. No. 81-754 (1950); Pub. L. No. 89-487 (1967).

² See, e.g., letter from Hon. Henry Waxman, Chairman, Comm. on Oversight & Gov't Reform, to Hon. Michael Astrue, Comm'r, U.S. Soc. Sec. Admin., *et al.* (Apr. 12, 2007); letter from Hon. Darrell Issa, Chairman, Comm. on Oversight & Gov't Reform, to Hon. Jeffrey Zients, Acting Dir. for Mgmt., Office of Mgmt. & Budget, *et al.* (Dec. 13, 2012); MAJORITY STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 114TH CONG., FOIA IS BROKEN: A REPORT (2016).

³ Pub. L. No. 113-187 (2014); Pub. L. No. 114-185 (2016).

⁴ OFFICE OF INSPECTOR GEN., COMMODITY FUTURES TRADING COMM'N, REVIEW OF THE COMMODITY FUTURES TRADING COMMISSION'S OVERSIGHT AND REGULATION OF MF GLOBAL, INC. (May 16, 2013).

⁵ See Carol D. Leonnig and Joe Stephens, *Energy Department loan program staffers were warned not to use personal e-mail*, WASH. POST, Aug. 14, 2012, http://articles.washingtonpost.com/2012-08-14/politics/35490043_1_personal-e-mail-e-mails-email.

Where a federal employee conducts any business related to the work of the government from a non-governmental email account, such as a personal email account, the Federal Records Act requires that the employee copy their official account or forward the record to their government email account within 20 days.⁶ Official business must be conducted in such a way as to preserve the official record of actions taken by the federal government and its employees.

Recent news reports suggest federal employees may increasingly be turning to new forms of electronic communication, including encrypted messaging applications like Signal, Confide, and WhatsApp, that could result in the creation of federal records that would be unlikely or impossible to preserve.⁷ The security of such applications is unclear.⁸ Generally, strong encryption is the best defense against cyber breaches by outside actors, and can preserve the integrity of decision-making communications. The need for data security, however, does not justify circumventing requirements established by federal recordkeeping and transparency laws.

To assist the Committee in better understanding your agency's policies on these issues, please provide the following information as soon as possible, but by no later than March 22, 2017:

1. Identify any senior agency officials who have used an alias email account to conduct official business since January 1, 2016. Include the name of the official, the alias account, and other email accounts used by the official to conduct official business.
2. Identify all agency policies referring or relating to the use of non-official electronic messaging accounts, including email, text message, messaging applications, and social media platforms to conduct official business, including but not limited to archiving and recordkeeping procedures.
3. Identify all agency policies referring or relating to the use of official text message or other messaging or communications applications, and social media platforms to conduct official business, including but not limited to archiving and recordkeeping procedures.
4. Identify agency policies and procedures currently in place to ensure all communications related to the creation or transmission of federal records on official electronic messaging accounts other than email, including social networking platforms, internal agency instant messaging systems and other communications applications, are properly captured and preserved as federal records.

⁶ 44 U.S.C. § 2911 (2017).

⁷ Andrew Restuccia, Marianne Levine, and Nahal Toosi, *Federal workers turn to encryption to thwart Trump*, POLITICO, Feb. 2, 2017, <http://www.politico.com/story/2017/02/federal-workers-signal-app-234510>; Jonathan Swan and David McCabe, *Confide: The app for paranoid Republicans*, AXIOS, Feb. 8, 2017, <https://www.axios.com/confide-the-new-app-for-paranoid-republicans-2246297664.html>.

⁸ Sheera Frenkel, *White House Staff Are Using A "Secure" App That's Not Really So Secure*, BUZZFEED NEWS, Feb. 16, 2017, <https://www.buzzfeed.com/sheerafrenkel/white-house-staff-are-using-a-secure-app-thats-really-not-so>.

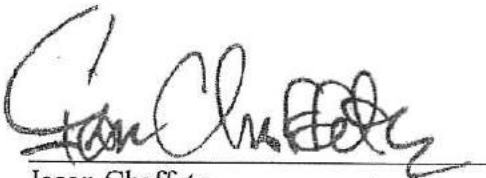
5. Explain how your agency complies with FOIA requests that may require searching and production of documents stored on non-official email accounts, social networking platforms, or other messaging or communications.
6. Provide the status of compliance by the agency with the Managing Government Records Directive issued by the Office of Management and Budget on August 24, 2012.⁹

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2471 of the Rayburn House Office Building. The Committee prefers, if possible, to receive all documents in electronic format. An attachment to this letter provides additional information about responding to the Committee's request. Please note that Committee Rule 16(b) requires counsel representing an individual or entity before the Committee or any of its subcommittees, whether in connection with a request, subpoena, or testimony, promptly submit the attached notice of appearance to the Committee.

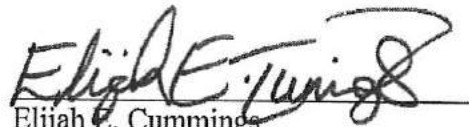
The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and may at "any time" investigate "any matter" as set forth in House Rule X.

For any questions about this request, please have your staff contact Jeff Post of the Majority staff at (202) 225-5074 or Krista Boyd of the Minority staff at (202) 225-9493. Thank you for your attention to this matter.

Sincerely,



Jason Chaffetz
Chairman



Elijah E. Cummings
Ranking Member

Enclosures

⁹ Jeffrey D. Zients, Acting Director, Office of Management and Budget and David S. Ferriero, Archivist of the United States, National Archives and Records Administration, *Managing Government Records Directive* (Aug. 24, 2012) (M-12-18).



ADMINISTRATIVE COMMUNICATIONS SYSTEM U.S. DEPARTMENT OF EDUCATION

DEPARTMENTAL DIRECTIVE

OM: 6-103

Page 1 of 25 (05/04/2016)

Distribution:
All Department of Education
Employees

Signed by: Andrew Jackson
Assistant Secretary for Management

Records and Information Management Program

Table of Contents

I.	Purpose	2
II.	General Policy	3
III.	Authorization.....	8
IV	Applicability.....	11
V.	Definitions and Acronym Glossary.....	11
VI	Responsibilities.....	15
VII.	Requirements	21

For technical information regarding this document, please contact Sherry Smith via email or at 202-401-0902.

Supersedes: OM: 6-103 "Records and Information Management Program", dated 08/07/2012.

I. Purpose

This Directive establishes the overall policies and procedures to be followed by the U.S. Department of Education's (ED) Principal Offices (POs), employees, and contractors in complying with the requirements of the *Federal Records Act of 1950 as codified in 44 U.S.C. Chapters 29, 31, and 33, as revised by the Presidential and Federal Records Act Amendments of 2014 (Amendments to the Federal Records Act of 2014) and the National Archives and Records Administration (NARA) implementing regulations contained in 36 CFR 1220 through 1239* for establishing and maintaining a records management program in administrative and mission-related activities that is compliant with the relevant statutes, regulations, NARA-issued guidance, and Departmental records management policies.

This Directive also authorizes the issuance of a Records and Information Management Manual (Records Manual), for Principal Office Records Liaison Officers (RLOs) and a Records Management Handbook for all employees which includes processes and procedures for specific categories of records and records management activities.

However, this Directive does not address all information resources management requirements affecting records management. This Directive should be considered in context with other ED Information Resource Management (IRM) policies located at the Records and Document Management Division on connectED at, <https://connected.ed.gov/om/records/SitePages/Default.aspx>

A. The specific objectives of the records management program are:

1. To establish responsibilities and requirements for developing, implementing and maintaining an efficient and effective, NARA-compliant records management program at ED.
2. To facilitate ED's transition to full electronic recordkeeping as the foundation of an electronic records management program in compliance with the provisions of the Presidential Memorandum dated November 28, 2011, *Managing Government Records* and the OMB/Directive M-12-18, *Managing Government Records*.
3. To provide support for ED's mission of promoting educational excellence for all Americans through:
 - a. Ensuring that every ED senior official, employee, and contractor is aware that they have specific records management responsibilities imposed by statute and regulation, and to provide training in how to meet those responsibilities;

- b. Creating and preserving adequate and proper documentation of ED activities, organization functions, policies, decisions, procedures, and essential transactions;
 - c. Appropriate access, retrieval, maintenance, and use of ED records in all formats; and
 - d. Proper records retention and disposition of ED records in all formats.
- B. To comply with the Federal Records Act, and applicable statutes, authorities, and regulations as listed in the Authorization section. Proper records management helps assure efficient and effective administration of programs, minimizes costs, fulfills legal responsibilities, provides an adequate audit trail, and records the history and intent of public policy.
- C. To preserve historical information, thereby enabling ED employees, ED contractors, and their successors to retrieve information needed to make informed decisions.
- D. To establish an essential records program that identifies, protects, and provides ready access to records necessary to ensure continuity of essential Departmental activities in the event of a national disaster or emergency.
- E. To promote open government and support the principals of transparency in government.

II. General Policy

It is the policy of ED to create, preserve, maintain, use, and dispose of Federal records in compliance with the requirements of the Federal Records Act of 2014, as amended and applicable NARA regulations, and to ensure access to information by ED officials, and the public, as appropriate. This policy covers all records, regardless of format or location that meet the criteria for Federal records. Unstructured electronic records (see definition) will either be maintained in a NARA-compliant electronic recordkeeping system or printed to paper for recordkeeping. POs are authorized to organize their shared drives as recordkeeping systems, (in accordance with NARA guidelines) as an interim measure until the Enterprise Electronic Records Management System (EERMS) is implemented within their office. Structured electronic records, such as data sets, will be managed as Federal records within their system of origin.

ED and POs will establish and maintain effective and efficient practices for the management of Federal records in all formats. Principal Officers and program and administrative managers have the ultimate functional responsibility for

implementing ED records management policies and procedures in their operational areas.

Each PO is responsible for ensuring that its program records are covered by and managed in accordance with appropriate retention and disposition schedules, and imposition any corresponding litigation, Freedom of Information Act (FOIA) or oversight holds. Records not covered by ED's Records Retention and Disposition Schedules or NARA-issued General Records Schedules (GRS) must be scheduled by application to NARA for legal disposition authority. Unscheduled records shall not be destroyed or deleted, whether in paper or electronic format.

A. Electronic Messaging

Electronic messages, as defined by the Amendments to the Federal Records Act of 2014, shall be managed in accordance with the provisions of the Amendment, including those records created or received by mobile devices.

Personal email accounts shall not be used for the conduct of government business. However, if a Federal record is created or received in a personal email account, it shall be forwarded to the ED email system or printed to paper for recordkeeping within 20 days (with the exception of Saturdays, Sundays, and legal public holidays). If a Federal record is created or received as an electronic message, it shall either be forwarded to the ED email system by the individual user or captured centrally as part of network operations related to the ED network.

ED shall not destroy any email until receiving NARA disposition approval for its use of NARA's Capstone approach. This approach may involve use of GRS 6.1 for disposition or by applying to NARA for independent disposition authority through submission of ED-specific records retention schedules.

The Office of the Chief Information Officer (OCIO) is responsible for managing electronic messaging records with the exception of records created and maintained on individual mobile devices, whether government furnished telephones or tablets or privately owned cell phones registered through the Bring Your Own Device program.

Principal Offices are responsible for properly managing electronic messages created by use of social media applications.

The individual owner or user is responsible for managing electronic messages such as text messages that are created or received using the mobile devices discussed above. Text messages that qualify as federal records must be forwarded to ED's email system for recordkeeping purposes. Please refer to

the applicable Job Aid posted on the Records Management website at: <https://connected.ed.gov/om/records/SitePages/Tools.aspx> for more information about how to capture text messages in the email system.

B. Electronic Records Management Requirements

POs are authorized to establish electronic recordkeeping systems (as defined by NARA) on their shared drive as a substitute for "print and file." POs that utilize their shared drive as a recordkeeping system are required to meet the requirements of NARA Bulletin 2012-02 *Guidance on Managing Content on a Shared Drive*.

C. Internal Evaluations of Records Programs

POs shall conduct an annual internal evaluation (records management self-assessment) of their records management programs to certify that their programs are operating in compliance with NARA and ED policies and procedures. Principal Office Program Records Officials (PRO) will submit the annual certification to ED's Records Officer by December 31st of each year. POs will conduct, in conjunction with ED's Records Officer, an in-depth evaluation of their records management program every three (3) years (triennial records management self-assessment). This in-depth review will consist of, but not be limited to, records sampling, record inventories, updates to program record schedules, and personalized training. POs will submit an annual corrective action plan to ED's Records Officer that addresses any deficiencies identified in the annual internal evaluation and/or the triennial review. The POs designated RLOs are responsible for performing these evaluations. Reviews and evaluations will be conducted in accordance with NARA regulations and, "NARA Records Management Self-Evaluation Guide," and ED's records management policies and procedures.

D. Safeguarding Records

Records collected, created, or maintained by ED shall be safeguarded commensurate with the risk and magnitude of the harm that would result to ED from the disruption or loss of access to or use of information, the unauthorized disclosure of information, and the unauthorized modification or destruction of information in accordance with the security categorizations set forth in Federal Information Processing Standards (FIPS) Publication 199. Safeguards shall be adopted to provide protection for information that is restricted from disclosure by the Privacy Act, the Family Educational Rights and Privacy Act, the Computer Security Act, the Federal Information Security Management Act, or other statutes, regulations, Executive Orders, or authorities. In addition, POs shall incorporate in their records management activities all applicable ED information security policies and measures,

including the requirements contained in the Handbook for Information Assurance Security Policy (Handbook OCIO-01) and the Controlled but Unclassified Information (CUI) program.

E. Records Ownership

All records created or received by an official, employee or contractor of ED in the course of conducting Federal Government business are the property of ED, wherever the record resides (for example, in a personal email account). No person attains a proprietary interest in any record that he/she may create, provide input into, or acquire custody or possession of, by virtue of his/her position as an official, employee, or contractor. Materials that are entirely personal are not "records" for purposes of Departmental records management requirements. Personal materials shall at all times be maintained separately from a POs records, and may be removed by an employee or contractor of ED.

F. Records Removal

Removal of documentary materials by a separating employee or contractor must be approved in accordance with the provisions of this Directive to ensure that ED's ability to claim privileges during litigation, to apply FOIA exemptions, and to protect confidential information is not diminished, or waived. Contracting Officer's Representatives (CORs) are responsible for ensuring that departing contractors do not remove any ED records. ED Records Management will work with CORs to develop a process and procedures for certifying departing contractors do not remove ED materials.

Destruction of records is authorized only when conducted in compliance with ED's records disposition schedules, as approved by the Archivist of the United States, and the GRS, issued by NARA as described in 36 CFR, Section 1230.10. Criminal penalties may be imposed for the willful and unlawful destruction, damage, or removal of Federal records, as described in 18 U.S.C. Section 2071.

G. Essential Records Program (Formerly the Vital Records Program)

The establishment of an essential records program is a subset, yet integral part of a Records Management Program. ED is following NARA guidance that renames these records as essential, rather than vital.

The Essential Records Program identifies, protects, and provides ready access to vital records necessary to ensure continuity of essential ED activities in the event of a national, regional, or local disaster or emergency.

1. To identify and protect the records and information necessary to continue key operations; protect the legal and financial rights of ED, its employees or the public; and protect the records deemed critical for the continuity and/or resumption of mission-essential functions.
 - a. The goals of the program are to ensure that emergency operating records critical to the continuity of essential Departmental activities during a national emergency are available in the event the site is activated during a national emergency;
 - b. To safeguard rights and interests records essential to the preservation of the legal rights and interests of individual U.S. citizens, and the Federal Government, including those records that limit or prohibit disclosure;
 - c. To ensure that essential records are evaluated on the basis of whether they are essential in the conduct of emergency operations or in the protection of the rights and interests of citizens, and the Federal Government;
 - d. To ensure that the records are adequate to carry out ED's critical functions and are available for use by individuals other than those who would generally use them;
 - e. To ensure that records are easily retrievable and that they are maintained in usable conditions;
 - f. To ensure that the current inventory of records located at the relocation site is readily accessible; and
 - g. To inform all personnel of their responsibilities under this program.
2. Under the Essential Records Program each PO shall:
 - a. Comply with and support the Essential Records Program, and ensure that their respective emergency operating records and legal and financial rights records vital to the continuity of essential ED activities are properly identified, safeguarded, and accessible;
 - b. Review, update, and revise their Essential Records Plans by reviewing the vital records, as needed, but not less than annually (subject to periodic reviews by Departmental Records Officer (DRO) or his/her designated representative);
 - c. Ensure that essential records are evaluated on the basis of their essentiality in carrying out emergency operations or in protecting the

rights and interests of citizens and Government and not based on their value as long-term temporary or permanent records;

(NOTE): The records must be available and sufficient enough so that anyone at ED's Continuity of Operations (COOP) sites or other off-site locations can appropriately access and interpret the information. It is important to remember that individuals at COOP sites accessing the information may not be familiar with the information so records must be clear and concise.)

- d. Ensure that their essential records are preserved, catalogued, and easily retrievable in usable condition in the appropriate medium for ready access at the ED COOP sites or other appropriate off-site locations;
- e. Coordinate with the DRO when transferring emergency operating records and legal and financial right records to the ED COOP sites or other appropriate off-site locations; and
- f. Consider the informational content of records series and electronic records systems when identifying vital records such as emergency plans and related records, and those records that would be needed to continue operations and protect legal and financial rights.

III. Authorization

The Federal Records Act US CODE: Title 44, CHAPTER 31—RECORDS MANAGEMENT BY FEDERAL AGENCIES, and the relevant requirements of Title 36, Code of Federal Regulations (CFR), 1220 through 1239, contain the statutory and regulatory requirements for all Federal records management programs, including the recent Amendments to the Federal Records Act of 2014. NARA administers the records management program for the Federal Government. NARA's regulations on records creation, maintenance, and disposition are set forth in Subchapter B of 36 Code of Federal Regulations Chapter XII, as well as in numerous NARA bulletins, memorandums, and directives.

Agencies are required to integrate records management into their overall information resources management program (36 CFR 1222 and OMB Circular A-130, *Management of Federal Information Resources*). The controlling statutes, regulations, Office of Management and Budget (OMB) Circulars and Executive Orders appear below:

United States Code

- **5 U.S.C. Chapter 5, Subchapter II – Administrative Procedure**
 - § 552. Public information; agency rules, opinions, orders, records, and proceedings (Freedom of Information Act, as amended)
 - § 552a. Records maintained on individuals (Privacy Act of 1974, as amended)
 - § 553. Rulemaking (Administrative Procedures Act)
- **18 U.S.C. Chapter 101 – Records and Reports**
 - § 2071. Concealment, removal, or mutilation generally
- **40 U.S.C. Subtitle III – Information Technology Management (Clinger-Cohen Act of 1996)**
- **44 U.S.C. Chapter 21 – National Archives and Records Administration**
- **44 U.S.C. Chapter 29 – Records Management by the Archivist of the United States and by the Administrator of General Services**
- **44 U.S.C. Chapter 31 – Records Management by Federal Agencies (Federal Records Act)**
- **44 U.S.C. Chapter 33 – Disposal of Records (Federal Records Disposal Act)**
- **44 U.S.C. Chapter 35 – Coordination of Federal Information Policy (Paperwork Reduction Act of 1980, as amended; Paperwork Reduction Reauthorization Act of 1995; and Government Paperwork Elimination Act)**

Code of Federal Regulations

- **5 CFR Chapter III, Subchapter B – OMB Directives**
 - Part 1320. Controlling Paperwork Burdens on the Public
- **36 CFR Chapter XII, Subchapter B – Records Management**
 - Part 1220. Federal Records; General
 - Part 1222. Creation and Maintenance of Records
 - Part 1223. Managing Vital Records

- Part 1224. Records Disposition Program
- Part 1225. Scheduling Records
- Part 1226. Implementing Disposition
- Part 1227. General Records Schedule
- Part 1228. Loan of Permanent and Unscheduled Records
- Part 1229. Emergency Authorization to Destroy Records
- Part 1230. Unlawful or Accidental Removal, Defacing, Alteration or Destruction of Records
- Part 1231. Transfer of Records from the Custody of One Executive Agency to Another
- Part 1232. Transfer of Records to Records Storage Facilities
- Part 1233. Transfer, Use, and Disposition of Records in a NARA Federal Records Center
- Part 1234. Facility Standards for Records Storage Facilities
- Part 1235. Transfer of Records to the National Archives of the United States
- Part 1236. Electronic Records Management
- Part 1237. Audiovisual, Cartographic, and Related Records Management
- Part 1238. Microform Records Management
- Part 1239. Program Assistance and Inspections

OMB/NARA Directives

M-12-18 Managing Government Records

OMB Circulars

- **OMB Circular A-123** – Management's Responsibility for Internal Control
- **OMB Circular A-130** – Management of Federal Information Resources

Executive Orders

- **Executive Order 10346** - Preparation by Federal Agencies of Civil Defense Emergency Plans
- **Executive Order 12656** - Assignment of Emergency Preparedness Responsibilities
- **Executive Order 13231** - Assignment of Emergency Preparedness Responsibilities
- **Presidential Memorandum** - *Managing Government Records* dated Nov 28, 2011

IV **Applicability**

This Directive applies to all ED employees and contractors who have a network account or who otherwise create or receive records as an agent of ED, and covers all ED records regardless of format or medium, as defined in the Amendments to the Federal Records Act of 2014.

V. **Definitions and Acronym Glossary**

The following records management terms are extracted from 36 CFR, Part 1220 and the Amendments to the Federal Records Act of 2014.

- Administrative records** are records that reflect routine, transitory, and internal housekeeping activities relating to subjects and functions common to all offices. Examples include training, personnel, and travel reimbursement files. Administrative records in conjunction with program records comprise the universe of agency records.
- Amendments to the Federal Records Act and the Presidential Records Act of 2014** modernize the definition of Federal records to include electronic records.
- Annual Internal Evaluation** is a formal evaluation to measure the effectiveness of records management programs and practices, and to ensure compliance with NARA regulations in this subchapter.
- Capstone** is an approach developed by NARA as a means of managing and scheduling email records where final disposition is determined by the role or position of the account user, rather than the content of the individual email.
- Continuity of Operations (COOP)** plan is a contingency action plan which provides the capability for a Department and/or Agency to continue

operations during a crisis which renders the organization's headquarters unusable.

- F. **Controlled Unclassified Information (CUI)** is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.
- G. **Disaster** refers to an unexpected occurrence inflicting widespread destruction and distress and having long-term adverse effects on agency operations.
- H. **Disposition Schedules** are mandatory disposition instructions that provide continuous authority to dispose of recurring series or systems of records, or to transfer them to the National Archives and its national network of Federal Records Centers. ED's disposition schedules are contained with the ED Records Retention and Disposition Schedules.
- I. **Documentary Material** is a collective term for records and non-record materials that refers to all media on which information is recorded, regardless of the nature of the medium or the method or circumstances of recording (36 CFR 1220.18).
- J. **Electronic messaging** means electronic mail and other electronic messaging systems (text messaging, instant messaging, chat, voicemail messaging, social media or mobile device applications) that are used for the purposes of communicating between individuals.
- K. **Federal Records Act of 1950**, as amended, establishes the framework for records management programs in Federal agencies.
- L. **Information resources management** means the process of managing information resources to accomplish agency missions. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and information technology.
- M. **File Plan** is (1) a plan designating the physical location(s) at which a PO's files are to be maintained, the specific types of files to be maintained there, and the organizational element(s) having custodial responsibility; or (2) a document containing the identifying number, title or description, and disposition of files held in an office.
- N. **General Records Schedules (GRS)** are mandatory disposition instructions issued by NARA for temporary administrative records that are common to most Federal agencies.

- O. **Litigation and Oversight Holds** stipulate that all records that may relate to a legal or Congressional oversight action involving ED must be retained. This requirement ensures that the applicable records are available for the discovery process prior to litigation. ED must preserve records when it learns of pending or imminent litigation, or when litigation is reasonably anticipated. Litigation holds prevent the spoliation (e.g. destruction, alteration, or mutilation of evidence) which can have a negative impact in litigation.
- P. **National Archives and Records Administration (NARA)** establishes policies and procedures for managing U.S. Government records. NARA assists Federal agencies in documenting their activities, administering records management programs, scheduling records, and retiring non-current records to Federal records centers, and conducts periodic evaluations of agency compliance.
- Q. **Non-record materials** are U.S. Government-owned informational materials excluded from the legal definition of records. This includes extra copies of documents kept only for convenience of reference, stocks of publications and processed documents, and library or museum materials intended solely for reference or exhibition.
- R. **Permanent records** are those records appraised by NARA as having sufficient historical or other value to warrant continued preservation by the Federal Government beyond the time they are needed for administrative, legal, or fiscal purposes. Permanent records will be transferred to the physical and legal custody of NARA in accordance with the instructions contained in the relevant records disposition schedule.
- S. **Personal papers** are documentary materials belonging to an individual that are not used to conduct agency business. These papers are related solely to an individual's own affairs or used exclusively for that individual's convenience. They must be clearly designated as personal and kept separate from the Department's records.
- T. **Program records** refer to records created, received, and maintained by the Department in the conduct of its mission functions for which the Department is accountable. The term is used in contrast to administrative records. Program records in conjunction with administrative records comprise the universe of agency records.
- U. **Structured (data) records** are information with a high degree of organization, such that inclusion in a relational database is seamless and readily searchable by simple, straightforward search engine algorithms or other search operations and that meet the criteria as Federal records. Record-keeping requirements are statements in statutes, regulations,

Directives, handbooks, or guidance that provide general and specific information on particular records to be created and maintained by the Department.

- V. **Records** include all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the United States Government or because of the informational value of data in them. (44 USC 3101, Definition of Records).
- W. **Recorded Information** includes all forms of records, regardless of format or characteristics, including information created, manipulated, communicated, or stored in physical, digital, or electronic form, including metadata.
- X. **Records management program** refers to the planned coordinated set of policies, procedures, and activities needed to manage an agency's or department's recorded information. Encompasses the creation, maintenance and use, and disposition of records, regardless of media. Essential elements include issuing up-to-date program Directives, properly training those responsible for implementation, and carefully evaluating the results to ensure adequacy, effectiveness, and efficiency.
- Y. **Retention period** is the period of time that records are to be kept in accordance with NARA-approved records disposition schedules.
- Z. **Temporary records** are records approved by NARA for disposal, either immediately or after a specified retention period.
- AA. **Unstructured Data (or unstructured information)** refers to information that either does not have a pre-defined data model or is not organized in a pre-defined manner. Unstructured information is typically text-heavy, but may contain data such as dates, numbers, and facts as well and that meet the criteria as Federal records.
- BB. **Essential Records**, previously called Vital Records, are essential agency records needed to meet operational responsibilities under national or regional emergency or disaster conditions. Previously called Vital Records.

Acronym Glossary

- ARCIS – Archives and Records Centers Information System

- DRO – Departmental Records Officer
- EIS – Electronic Information System
- ERA – Electronic Records Archive
- ERM – Electronic Records Management
- EERMS – Enterprise Electronic Records Management System
- FRA – Federal Records Act
- FRC – Federal Records Center
- GRS – General Records Schedules
- NARA – National Archives and Records Administration
- OCPO – Office of the Chief Privacy Officer
- PRO – Program Records Official
- RLO – Records Liaison Officer
- RRO – Regional Records Official
- WNRC – Washington National Records Center at Suitland, Maryland

VI Responsibilities

- A. The **Secretary** shall ensure the creation and preservation of records that adequately and properly document the organization, functions, policies, decisions, procedures, and essential transactions of ED. Operational responsibility for this program is delegated to the **Assistant Secretary for Management** and re-delegated to the **Chief Privacy Officer**. **The Secretary shall designate a senior official to act as the Senior Agency Official for Records Management** as required by the Presidential Memorandum *Managing Government Records* dated November 28, 2011. **The Assistant Secretary for Management is the Senior Agency Official for Records Management.**
- B. The **Chief Privacy Officer** shall provide overall leadership, planning, supervision, guidance, direction and general oversight of ED's Records Management Program, and ensure its integration into the broader information resources management framework.

C. **Principal Officers and Program Directors shall** provide for the implementation of the records/information management program within their respective areas. They will:

1. Ensure that the objectives of ED's records management program are achieved;
2. Establish, implement, and sustain records management programs within their respective organizations, including a vital records program;
3. Ensure that staff, including contractors, are informed about and understand their responsibility for preserving and appropriately managing their records in all formats, including electronic messaging applications such as email, text messaging, instant messaging, chat, voicemail, social media or mobile device applications.
4. Ensure an annual internal evaluation and a triennial review of their PO's records management program is performed and certify that it is in compliance with NARA regulations and ED policies;
5. Ensure that permanent records are preserved and temporary records are transferred to off-site storage or destroyed promptly according to NARA-approved records disposition schedules;
6. Ensure that removal of documentary materials by separating ED employees is in accordance with the provisions of this Directive; CORs are responsible for ensuring that departing contractors do not remove any ED records.
7. Ensure appropriate records management training for PROs, RLOs, and all other Department employees commensurate with their level of responsibility for records management;
8. Provide adequate staff resources to support records management processes within their respective organizations by assigning the following roles and responsibilities to designated staff:
 - a. A senior-level PRO with signature authority to approve records issues for the program and serve as the liaison with the Department's Records Officer;
 - b. At least one RLO to provide day-to-day administration of an organization's records management program under the direction of the PRO; and

c. Regional Records Officials (RROs), when designated, will assume local responsibilities corresponding to those of the PO's RLO.

9. Provide names and contact information, and updates as changes occur, for the designated PROs, RROs, and RLOs to the Department's Records Officer, Privacy, Information, and Records Management Services, Office of Management.

D. Program Records Officials, Regional Records Officials, and Records Liaison Officers. The PROs are responsible for the following program activities supporting the Department Records Management Program. Except for the items marked "PRO," these activities may be delegated to the RLOs and the RROs for their individual offices and sites.

1. Coordinate the records management program activities, including an essential records program in their respective organizations to ensure compliance with this Directive through the designated RLOs and RROs. (PRO);
2. Identify program-specific records and ensure they are covered by a NARA approved records disposition schedule;
3. Ensure that permanent records are preserved and temporary records are transferred into off-site storage or destroyed promptly according to NARA-approved records disposition schedules;
4. Ensure that record-keeping requirements are established and kept current and that staff is kept abreast of any changes to these recordkeeping requirements;
5. Review and approve or disapprove requests for removal of documentary materials by separating employees, and forward in a timely manner, the completed Documentary Materials Removal/Non removal Certification forms to ED's Records Officer. This process may also be performed electronically via email.
6. Ensure that CORs provide oversight for contractor departures to prevent removal of ED records;
7. Ensure that all personnel with records management responsibilities receive appropriate records management training. (PRO);
8. Ensure that RLOs obtain appropriate NARA records management training and earn the NARA RM Certificate;

9. Ensure that ED's Records Management Program provisions and standards are included in the scope and planning for electronic information systems. (PRO);
10. Ensure that records are maintained cost effectively and that records storage facilities meet the requirements of 36 CFR 1234. (PRO);
11. In conjunction with ED's Records Officer, ensure the development and implementation of a PO file plan; and
12. Ensure that departing employees and contractors identify and transfer all Federal records in their custody to the designated custodian of the program files, i.e., either to the RLO or the person assuming responsibility for the work.

E. The Departmental Records Officer (DRO), OCPO shall:

1. Develop policies and procedures related to the requirements of this Directive and provide advice and consultation to POs in furtherance of its implementation;
2. Provide overall leadership for ED records management activities, as required by Federal laws and regulations which are specified in the Authorization section of this Directive;
3. Make available guidance, expertise, technical assistance, and training to staff in all aspects of the records management program;
4. Serve as ED's point of contact with NARA, other Federal agencies, and the public sector for issues related to ED's records management program;
5. Evaluate program effectiveness through periodic reviews of PO's records management activities;
6. In conjunction with PO records officials, develop records retention and disposition schedules and once completed, serve as ED's official point of contact for such schedules;
7. Coordinate with PROs in the implementation of ED's Records Management Program throughout ED;
8. Coordinate with PROs in the implementation of the documentary materials removal process for separating employees; Coordinate with CORs to ensure that contractors do not remove any ED records;

9. Ensure that the records management program has provided a records management clause for use in contracts where ED records are created and or maintained
 10. Review and approve or disapprove requests for removal of documentary materials by Presidential appointees; and
 11. Conduct records management exit briefings for Presidential appointees and other senior officials as requested.
- F. The **Office of Inspector General (OIG)** shall assist in determining the retention of Department records that may be needed for internal audit purposes. The OIG shall be informed by the Departmental Records Officer in instances where records are removed from ED's physical or legal custody without authorization so steps may be taken to regain custody of the records consistent with authorities in the Inspector General Act.
- G. The **Office of the General Counsel (OGC)** is responsible for the litigation hold process. OGC shall notify ED's Records Officer when a moratorium on records disposition is needed for litigation, oversight or other legal matters. OGC will support the submission of ED's records disposition schedules by reviewing them for legal sufficiency before submittal. OGC also provides legal advice on the laws and regulations related to the records and information management program. This includes coordination with the DRO to ensure compliance with recordkeeping requirements, determination of retention periods, and implementation of authorized disposition instructions for system data and documentation.
- H. The **Chief Information Officer** shall ensure that records management requirements are incorporated into the ED system development life cycle methodology as part of managing the information life cycle, and that NARA approved records retention and disposition schedules for electronic information systems and other electronic records, such as email, are properly implemented.
- I. **Program Managers** shall ensure that their programs are properly documented, and that records created by their programs are managed according to Federal law and regulations (see Authorizations section, and the provisions of this Directive).
- J. **Information System Managers** shall oversee the creation and use of electronic records according to Federal regulations and Departmental policy and ensure that recordkeeping functionality is developed for all information systems managing electronic records. This includes coordination with ED's Records Officer to ensure compliance with record-keeping requirements,

determine retention periods, and implement authorized disposition instructions for system data and documentation. Systems managers shall also coordinate with PROs when developing business cases for the Investment Review Board as part of the Capital Planning and Investment Control (CPIC) process to ensure that electronic records management requirements are incorporated into system design and development.

- K. **Information Technology Managers** shall notify the information system managers and PROs of technology changes that would affect access, retention, or disposition (archiving or disposing) of records in electronic information systems.

L. **All Department employees and contractors shall:**

1. Complete annual online records management awareness training; contractors shall send an email to their COR certifying that they have completed the training.
2. Conduct work in accordance with Federal records management regulations and ED's records management policies and procedures;
3. Create and maintain adequate and proper documentation (Federal records) for the work for which they are responsible; maintain records in a manner that facilitates access and retrieval regardless of format ;destroy records only in accordance with approved records retention and disposition schedules; and remove non-record materials from ED only after obtaining prior authorization;
4. File personal papers and non-record materials separately from official ED records;
5. Contact their PO's RLO or OM/OCPO if they have a question about the proper disposition of a record or any records management policy or procedure;
6. ED employees shall complete ED's "Documentary Materials Removal/Non removal Certification" form and submit to their PRO prior to separation from ED.
7. Capture and preserve in ED's email system any electronic messaging records that are not being managed centrally by OCIO.
8. Delete electronic files that are not Federal records as soon as they are no longer needed.

VII. Requirements

A. ED Records Network

1. POs shall appoint a senior-level PRO with signature authority to assume responsibility and accountability for the PO records management program;
2. POs shall appoint Headquarters RLOs and RROs in the Regions to implement the records management program; and
3. POs shall provide the names, titles, and telephone numbers, and changes as they occur, of those designated as PROs, RLOs, and RROs to ED's Records Officer.

B. Records Creation

1. Official records shall be created that are sufficient to ensure adequate and proper documentation of all of ED's functions, policies, decisions, procedures, and essential transactions; and
2. POs shall develop and disseminate to staff general and specific guidance for creating and maintaining records documenting their organization, functions, and activities. An example of such guidance is a description of the records that are required to be created and maintained for a specific activity included in the relevant program handbook or manual.

C. Records Maintenance and Use

1. In conjunction with guidance provided by ED's Records Officer, POs shall create and maintain current file plans that describe all categories of records created, received, and maintained, and disposed by personnel in the course of their official duties;
2. File plans shall be updated and a copy submitted to ED's Records Officer by March 31st of each year;
3. Records filing, indexing, and storage systems shall be designed, implemented and documented to the extent necessary to maximize their usefulness and facilitate access and retrieval for the life of the records;
4. Records shall be organized and indexed in a manner that permits employees and contractors with a need to access and retrieve the records to do so efficiently and effectively; and
5. Confidential and privacy-protected records shall be managed and safeguarded in accordance with any applicable Federal laws and

regulations requiring access to, protection of, or restrictions on the disclosure of these records as well as ED requirements governing access to and protection of confidential but unclassified information.

D. Records Retention and Disposition Schedules

1. POs shall retain and dispose of records in accordance with the NARA-approved records disposition schedules contained in ED's Records Retention and Disposition Schedules as posted on the connectED Records Management website;
2. Unscheduled records (records that are not covered by a NARA-approved records disposition schedule) may not be destroyed; and
3. Proposed records retention and disposition schedules for unscheduled records shall be submitted to ED's Records Officer for internal review and approval, and submission to NARA for review and approval.

E. Permanent Records

1. POs shall promptly transfer permanent records to the custody of NARA in accordance with the instructions of the relevant records disposition schedule;
2. POs shall ensure that information copies of SF-258s used to document transfer of permanent records to NARA are provided to ED's Records Officer in a timely manner;
3. Permanent records shall be created, maintained, and stored in media and formats that adhere to NARA standards in 36 CFR 1235.46;
4. Electronic records shall be transferred in a NARA approved format; and
5. Permanent electronic records shall be transferred to NARA in a software/hardware independent format.

F. Electronic Records Management

1. Unstructured, text-based electronic records shall be maintained in an NARA-compliant electronic recordkeeping system (such as a shared drive configured in compliance with NARA requirements) or printed, filed and retained as paper files.
2. Electronic information systems (EIS) that contain records will have records management processes and requirements incorporated into their design and operations, or the equivalent manual processes required to retain

their information. The following requirements shall be incorporated into the design and operations of an EIS containing ED records:

- a. The EIS shall allow for the creation and maintenance of records sufficient to meet the documentation needs of ED;
 - b. Records shall be stored and maintained in a manner that enables retrieval, access, and dissemination, if appropriate, for the life of the records;
 - c. Records within an EIS must be covered by a records disposition schedule;
 - d. The EIS must be capable of deleting temporary or transitory records or transferring permanent records to NARA, in accordance with the requirements of the relevant records disposition schedule; and
 - e. Permanent electronic records must be created, maintained, and stored in media and formats that adhere to NARA standards.
3. POs planning to manage their records in electronic form must ensure that the records, particularly those incorporating an electronic signature, are legally sufficient for audit and other evidentiary purposes requiring trustworthy records. The electronic records must be created and maintained in compliance with the requirements of all pertinent Federal IRM laws and regulations, NARA and OMB guidance, and ED IRM policies.

G. Records Destruction

1. Records shall be destroyed in accordance with ED's NARA-approved records disposition schedules. Records owners shall determine before destruction whether or not the records must still be retained due to a litigation freeze, or other ongoing business purpose.
2. Records containing CUI information shall be destroyed appropriately by shredding or other secured methods in accordance with OCIO-15 *Handbook for the Protection of Sensitive Unclassified Information*.
3. Criminal penalties may be imposed for the willful and unlawful destruction of Federal records, as described in 18 U.S.C. Section 2071.

H. Records Retirement and Storage

1. POs will promptly retire inactive records to a NARA-approved records storage facility;

2. RLOs will timely provide an information copy of SF-135s and inventories or other paperwork used to document transfer of records to off-site storage to ED's Records Officer; and
3. Upon request by ED's Records Officer, RLOs will provide statistics on the volume and location of records stored off-site, including records stored at commercial records storage facilities.

I. Records Security and Privacy Protection

Employees and contractors shall manage records containing CUI or privacy-protected information accordance with applicable statutes, regulations, policies and procedures for the life cycle of the records, including OCIO-15 Handbook for the Protection of Unclassified Sensitive Information.

J. Records Training

1. ED's Records Officer will develop general records management awareness and training materials for all Department employees and contractors;
2. ED's Records Officer will develop and deliver ED-specific records management guidance for RLOs; and
3. PROs will ensure that RLOs obtain appropriate NARA records management training.

K. Removal of Documentary Materials by ED Employees. CORs will follow the procedures established by the contract and the ED Records Management program to ensure that records are turned over when contractor employees separate.

1. General Procedures for Removal of Documentary Materials
 - a. All records, originals and copies, are under the control of ED, regardless of how and by whom they were created or obtained;
 - b. Records of ED may not be removed under any circumstances. Non-record materials shall not be removed if this will create such a gap in the files as to impair the completeness of essential documentation. Indexes, or other finding aids, necessary for the use of the official records may not be removed;
 - c. Extra copies (photocopies, etc.) of records may be removed under certain circumstances. Prior to removal, it must be determined by OGC and OM/OCPO that no legal or policy reason exists for keeping

the information confidential and that the record copies, or other necessary copies, are available at ED. If the copy is of a document originating with another agency, the requirements of the originating agency must be determined (see Appendix B);

- d. Confidential but unclassified, or privacy-protected information may not be removed under any circumstances from ED; and
- e. Any violation of the statutory and regulatory limitations placed on removal of documentary materials by ED officials or employees who resign or retire will be forwarded to the appropriate officials, (e.g., Director of Information Assurance, Director of Security), who shall confer with the Inspector General regarding such violations.

2. Request to Remove Documentary Materials

- a. ED employees desiring to remove documentary materials must submit a written request to their PO PRO/RLO, listing the specific materials for which permission is required. All employees shall complete the *"Documentary Materials Removal/ Non-Removal Certification Form."* Email certification is also permitted.

L. Records Management Guidance

The Records Management office will periodically issue guidance documents in accordance with requirements established in NARA bulletins and other NARA issuances. These guidance documents are incorporated by reference in this Directive, and are binding upon POs records management programs. Guidance documents already issued include essential records, social media records, text messaging, and records management in cloud computing environments. All records management guidance documents are available to peruse on the Records Management website on connectED.



**ADMINISTRATIVE
COMMUNICATIONS SYSTEM
U.S. DEPARTMENT OF EDUCATION**

DEPARTMENTAL DIRECTIVE

OCIO: 3-109

Page 1 of 11 (03/20/2012)

Distribution:
All Department of Education
Employees

Approved by: Signed by
Winona H. Varnon
Principal Deputy Assistant
Secretary for Management
Delegated the Authority to Perform
the Functions and Duties of the
Assistant Secretary for Management

ED Social Media Policy

Table of Contents

I.	Purpose	2
II.	Policy	2
III.	Authorization	2
IV.	Applicability	3
V.	Responsibilities	4
VI.	Procedures and Requirements	5

I. Purpose

This directive provides guidance regarding the use of social media and associated web technologies. It follows the standards and guidelines for Federal government web usage, and complies with U.S. Department of Education (ED) policies. It is designed to support efforts to harness new technologies used to make ED more transparent, responsive, participatory, and collaborative.

II. Policy

"Social media" typically refers to use of web-based and mobile technologies to facilitate interactive information sharing, interoperability, and collaboration on the Internet, allowing users to interact and contribute content. Examples include Facebook, Twitter, YouTube, Flickr, as well as wikis, blogs, e-mail lists and bulletin boards. These technologies have the ability to increase information exchange, streamline processes, and foster productivity improvements across ED. For these reasons, ED supports the secure use by appropriate ED personnel of social media tools to enhance external communication, internal collaboration, and communication with stakeholders.

This directive outlines the measures and procedures needed to ensure compliance with laws and regulations that govern ED's online social media activities.

III. Authorization

- A. The Clinger-Cohen Act of 1996, Public Law 104-106, Title 41, United States Code (U.S.C.), Section 251 note, dated February 10, 1996.
- B. The E-Government Act of 2002, Public Law 107-347, 44 U.S.C. § 101 note, dated December 17, 2002.
- C. 5 Code of Federal Regulation (CFR) Part 2635, "Standards of Ethical Conduct for Employees of the Executive Branch."
- D. Executive Order 13526, Classified National Security Information, signed December 29, 2009, codified at 75 Federal Register (FR.) 707, dated January 5, 2010.
- E. Presidential Memorandum, "Transparency and Open Government", issued January 21, 2009, codified at 74 FR.4685, January 26, 2009.
- F. Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources", Revised Transmittal Memorandum No. 4, dated November 28, 2000.

- G. OMB Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002", dated September 26, 2003.
- H. OMB Memorandum M-10-22, "Guidance for Online Use of Web Measurement and Customization Technologies", dated June 25, 2010.
- I. OMB Memorandum M-10-23, "Guidance for Agency Use of Third-Party Websites and Applications", dated June 25, 2010.
- J. ED.gov Management and Publishing Policies,
<http://www2.ed.gov/internal/wwwstds.html>.
- K. Collection Scope and Criteria for Inclusion on Main ED Page of Links to Other Online Educational Resources,
<http://www2.ed.gov/about/contacts/gen/othersites/edrespol.html>.
- L. The Privacy Act of 1974, as amended.
- M. The Family Educational Rights and Privacy Act of 1974, as amended.
- N. The Children's Online Privacy Protection Act of 1998, as amended.
- O. The Federal Records Act of 1950, as amended.
- P. The Paperwork Reduction Act of 1995, as amended.
- Q. The Freedom of Information Act (FOIA) of 1966, as amended.
- R. The Federal Advisory Committee Act of 1972, as amended.
- S. Management of Social Media Records, Office of Management (OM).
- T. ED Personal Use of Government Equipment (April 17, 2006)
- U. ED Web 2.0 Records Management Guidance, June 2011
- V. OMB Memorandum for the Heads of Departments and Agencies, and Independent Regulatory Agencies, "Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act", dated April 7, 2010.
- W. Section 508 of the Rehabilitation Act of 1973, as amended.

IV. Applicability

This directive is intended to apply to all ED employees, staff, and offices using or considering use of social media technologies in an official capacity. It applies also to contractors working on behalf of ED as part of their duties.

V. Responsibilities

- A. The Office of Communication and Outreach (OCO) shall:
1. oversee all use of social media tools for ED external communications on publicly accessible sites;
 2. together with the Office of the Chief Information Office (OCIO), edit, revise, amend, or otherwise implement and maintain this directive according to its review guidelines; and
 3. provide leadership, analysis, coordination, and decision-making support on ED policies, plans, and key initiatives relating to websites and content.
- B. **-Information Assurance Services, OCIO** shall provide guidance on Information Technology (IT) risks, challenges (including cyber security threats and countermeasures, etc.), and possible resolutions for issues relating to ED's use of social media technologies and applications.
- C. **The Privacy, Information and Records Management Services (PIRMS), Office of Management (OM)** shall provide guidance and validate compliance of social media technologies relating to records management, privacy safeguards, and information collection and disclosure.
- D. **The Office of the General Counsel (OGC)** shall:
1. provide legal counsel for all technology-related initiatives;
 2. identify legal challenges and possible resolutions;
 3. validate that all use of social media complying with this ACS Directive is legally compliant with pertinent laws and regulations;
 4. negotiate any amendments to terms of service agreements; and
 5. provide policy advice on issues of social media usage and other issues addressed in this directive.
- E. **Web Sponsors (or users, including offices of ED)** shall be responsible for overall compliance with all aspects of this social media policy and must confer with OCO, OCIO, and OGC on issues relating to this directive. Accordingly, web sponsors are also responsible for all budget, implementation, personnel, management, authorization, and content matters related to the use of social media. The content owners on those sites and products are responsible for ensuring they conduct a reasonable review of the material to determine if any non-publicly releasable information, privacy information, or other restricted content is made available on their sites.

VI. Procedures and Requirements

- A. OCO and OCIO, in consultation with OGC, will select social media platforms that are appropriate for ED's goals and needs and operate effectively within ED's security environment. If an office has an unmet need and identifies an unauthorized social media platform that meets that need, the office must submit a written proposal to OCO stating the business need and requesting that the platform be reviewed for possible use at ED. This process applies regardless of hosting location of the social media platform.
- B. Important considerations, such as privacy and cyber security risks, are critical in determining when ED stakeholders can access or use social media. Because of the legal and security constraints placed on Federal agencies, the following policies apply to all uses of social media by ED staff:
 - 1. It is the policy of ED to ensure that all Principal Offices in ED using social media applications:
 - a. use social media applications only to distribute content that has been approved for distribution through other ED communications channels;
 - b. use social media applications to obtain general information including opinions, viewpoints, and input on general questions;
 - c. actively monitor discourse of social media content and remove comments that violate comments policies; and
 - d. provide links to equivalent information on an official ED website when it is not possible to make the information accessible on the native social media site.
 - 2. It is the policy of ED to ensure that all Principal Offices in ED using social media applications do not:
 - a. collect or retrieve personally identifiable information (PII) or information deemed sensitive and not otherwise available for public disclosure from social media applications;
 - b. make statements endorsing the use of, or affiliating with, any particular social media vendor or vendors (or related entities);
 - c. collect data on specific questions for the purpose of making policy decisions or conducting rulemaking activities; and
 - d. conduct ED business or state ED policy (e.g., social media platforms cannot be used to collect comments on ED's policies, proposed rules

or regulations, or other business activities. These must be submitted in accordance with procedures prescribed by existing rules, regulations and other guidance).

- C. Exceptions to these general policies must be approved by OCO in consultation with OCIO, OM and OGC.
- D. Use of all public-facing social media platform must be authorized by OCO in consultation with:
 - 1. Information Assurance, OCIO;
 - 2. Records and Documents Management Division, PIRMS, OM;
 - 3. Privacy Safeguards Division, PIRMS, OM;
 - 4. Information Collection Clearance Division, PIRMS, OM;
 - 5. FOIA Service Center (FSC), PIRMS, OM; and
 - 6. OGC.
- E. Use of social media platforms without authorization from the OCO can result in administrative actions in accordance with ED policies.
- F. Use of all non-public facing social media platforms must be authorized by the Chief Information Officer (CIO) in consultation with:
 - 1. Information Assurance, OCIO;
 - 2. Records and Documents Management Division, PIRMS, OM;
 - 3. Privacy Safeguards Division, PIRMS, OM;
 - 4. FOIA FSC, PIRMS, OM; and
 - 5. OGC.
- G. Use of social media platforms without authorization from the OCO can result in administrative actions in accordance with ED policies.
- H. All third party social media platforms must have a terms of service, license or other operating agreement in place after it has been reviewed and approved by OGC.

- I. ED may not use – on its own servers or an ED contractor's server - any social media product that uses "tracking technology" unless it complies with OMB Memorandum 10-22 and related guidance.
- J. Any ED use of social media that allows public comments must display a comment policy written in consultation with OGC. The office, initiative, or program must review and approve the comments before they are posted, if technologically possible and as staff capacity allows, in order to assure no comment violates that policy. If such review is not technologically possible, the comments must be monitored by the sponsoring office, initiative, or program - at least daily and as staffing capacity allows - to ensure that comments comply with the applicable comments policy. Generally, public comments must be relevant and must not contain racist, sexist, discriminatory, or profanity and they must not include privacy information, malicious links, or non-public information. Comments should also avoid activities that are prohibited in the Standards of Ethical Conduct for Employees of the Executive Branch.

Among other things, these standards prohibit:

- 1. engaging in vulgar or abusive language, personal attacks of any kind, or offensive terms targeting individuals or groups;
 - 2. endorsing of commercial products, services, or entities;
 - 3. endorsing of political parties, candidates, or groups; and
 - 4. lobbying members of Congress or any other legislative body using ED or any other appropriated resource.
- K. To the greatest extent possible, social media applications will allow users to post anonymously. ED will not use any social media products on its public-facing sites that require users to give their full names or other personally identifiable information. When the purpose is to obtain public feedback, ED will not use products that require a user to log in. ED may not use a third party product that requires a user to pay for access to Government information.
 - L. If ED's use of social media sites requires links to non-Government websites or products, the content should have limited commercial activity and should not imply an endorsement of any product or organization. Links should comply with ED's general linking policy. If technologically possible, language should be included on a social media product to disclaim any endorsement of non-Federal organizations or their products and services.

- M. When an ED employee is representing ED in an official capacity, ED is responsible for the content that employee publishes on blogs, wikis or any other form of user-generated media. ED employees should assume their communications are in the public domain, available for publishing or discussion in all forms of media. ED employees should remember that published content is persistent in the public domain.
- N. All official ED social media applications, profiles and accounts on public-facing sites must make their administrative login information available and accessible to the Senior Web Editor and New Media Director in OCO. This is to reduce the possibility of a single point of failure; provide continuity of service if a staff member working on a product, profile, or account leaves or is absent from ED; and provide the ability to track usage and gather data on the effectiveness of communications.
- O. All social media applications on public-facing sites must be branded in accordance with the branding guidelines established by OCO. Use of ED's seal must be approved and must conform to ED's policies.
- P. All social media content is subject to the Federal Records Act and National Archives and Records Administration (NARA) and ED records schedules and related requirements. The sponsor of any social media product must consult with their Principal Offices' Records Liaison Officer or the ED Records Management Program, PIRMS, OM to identify the appropriate records schedule that covers the content, and the content of the social media product must be disposed of in accordance with appropriate schedule requirements.
- Q. ED will not use social media to conduct surveys or to ask questions that collect information from non-Federal employees without approval under the Paperwork Reduction Act from OMB. ED may use social media to ask for opinions or general questions such as "what do you think?" Social media should not, however, be used to conduct official business around programs or policies. Social media may be used for customer service and communication with citizens and stakeholders unless an existing ED policy prohibits such use. Social media should not be used as the main or exclusive place for announcing ED policies and social media should not be used as a substitute for posting information on official ED websites. It may be used as an additional or supplemental means of information for citizens and stakeholders about ED news, developments, policies, and programs.
- R. No ED employee will post on a public-facing social media site any information exempt from release under FOIA (e.g., "deliberative or privileged" materials, materials relevant to a law enforcement investigation, etc.). ED employees may not speak for ED or discuss ED policies or programs unless authorized by OCO or unless such communications are otherwise protected by the Whistleblower Protection Act of 1989, as amended.

- S. OCO will maintain a list on ED.gov of public-facing social media sites that are approved by OCO for use by ED offices, programs, and initiatives. The list will include a disclaimer of any endorsement of non-Federal products and organizations and a statement of impartiality for products not in use by ED with an ed.gov email address to inquire about ED's participation in these products and services.
- T. Social media sites that are not public-facing, but are accessible to non-ED employees, must be governed by rules of behavior to which users must agree. Such rules must be written by the principal office sponsor of the social media site in consultation with OGC. These rules must include a statement prohibiting the release of information exempt under the provisions of FOIA.
- U. Access to social media sites is restricted through the ED network because these sites can increase exposure to privacy, cyber security, and related threats. Despite these risks, ED recognizes that social media sites offer an increasingly effective medium for communication. To take advantage of this opportunity while mitigating the risk, each principal office may request access to social media sites for a limited number of staff who need to access social media in order to do their jobs. This access is for "read only" purposes unless authorized by OCO, employees are not to post content or create official ED profiles on social media sites unless permission has been obtained in writing from OCO. To request access for particular staff members, the Assistant Secretary or his/her designee should send a request to OCO and OCIO. The request should include the names of ED staff needing access and a business justification – an explanation of why each individual needs access to social media sites, how they will use that access, what they hope to accomplish, and how the access will benefit the principal office. OCO will review requests and either authorize with restrictions and/or conditions, or decline access as soon as possible, but within 72 hours.
- V. If an office, initiative, or program believes that it needs to use a social media product, profile, account, or website to help achieve its goals, the senior officer may submit a business justification and plan of operations to OCO. The proposal must include a business justification and plan of operations - that is, what goals the office seeks to accomplish, whether the social media platform is a "good fit", and the plan of operations (who will do the posting and monitoring, what will be posted, and how often). OCO will also consider whether the proposal is clearly thought through and has a reasonable chance of achieving the desired outcomes; whether the proposed social media platform is right for the stated goals; and whether the proposal fits, complements, or overlaps with what another ED office is already doing or planning. OCO will also circulate the proposal to the appropriate ED experts for review (privacy, records management, security). OCO will respond to these proposals in a timely manner, generally within 10 working days. OCO

will coordinate with ED staff using social media and will issue and maintain policies and recommended best practices. Offices seeking to direct their contractors to use social media on their behalf should submit a proposal for such work to the OCO (as described above). The proposal should be submitted also to the appropriate staff in ED contract office.

W. Employees Personal Use of Social Media

1. Employees generally must not engage in personal social media use at the workplace during business hours and must not use Government equipment for personal social media. There is a limited personal-use exception that allows for the occasional use of Government equipment, provided that such use:
 - a. incurs only a negligible additional expense, if any, to ED;
 - b. does not distract from that employee's or other employees' ability to do their jobs;
 - c. occurs during off-duty hours (off-duty hours are the periods of time when an employee is not expected to be working, such as during a lunch break or before and after scheduled work hours), whenever possible; and
 - d. is not for the purpose of generating income for the employee or another individual (i.e., the employee is not using the equipment in connection with an initiative intended to make money).
2. Please refer to ACS directive OCIO: 1-104 "Personal Use of Government Equipment," which applies to the use of social media.
3. Employees may not state or imply that their personal use of social media sites is official. An employee who is authorized to speak for ED may not make official statements using personal social media accounts or profiles. If an employee's personal use of social media is otherwise likely to be considered as use on behalf of ED, employees should affirmatively state that their thoughts and opinions are their own and not the views of ED.
4. Similarly, if an employee encounters a situation in which public comment from ED appears warranted, and if the employee is not authorized to communicate official ED information to the public or media, the employee should contact the appropriate OCO representative.
5. Any employee who makes a public comment on topics or issues relating to ED during personal use of social media sites must disclose the relationship to ED (i.e., employee) and acknowledge that the response is

not reflective of official ED policy, actions, and that the employee is not speaking on behalf of ED. An employee may reference official ED statements or policy available to the public (i.e., by linking to ED press releases on ED.gov), as appropriate and applicable.

6. An employee may not release or discuss any non-public Government information as defined by Title 5, CFR, Section 2635.703. An employee may share all public information, and refer users to Government websites for additional guidance if it is appropriate and available.
7. ED staff who post content on any social media platform or website outside of ED's official online presence, on topics associated with ED must include a disclaimer such as "The postings are my own and do not necessarily represent ED's positions, strategies or opinions." ED staff shall never use or reference their official position when writing in a non-official capacity. If questions about this arise, OGC should be contacted for advice.
8. ED staff who have leadership responsibilities, by virtue of their positions, must consider whether personal thoughts they publish, even in clearly personal venues, may be misunderstood as expressing ED positions. They should assume that what they write will be read by their staff and those outside ED. The normal rules of behavior, code of conduct, and ethics rules apply to all activities discussed in this policy. ED staff should remember that a public blog is not the place to communicate ED policies to ED employees. Anything written on a publicly available social media platform or website should be assumed to be in the public domain. It can be published or discussed in all forms of media. There should be no expectation of privacy.
9. ED staff must follow copyright, trademark, and other laws. Sensitive information, such as protected acquisition and personally identifiable information must always be protected. Conversations that are meant to be pre-decisional or internal to ED should not be reported or published unless ED management gives permission to do so.
10. ED users will not use the same passwords for social media sites that are used to access ED resources.

JOINT GUIDANCE ON INSTANT MESSAGING AND TEXT MESSAGING PILOT PROGRAM

Issued by OCIO, OGC and PIRMS

I. PURPOSE

This joint guidance is issued by the Office of the Chief Information Officer; the Office of the General Counsel; and the Privacy, Information and Records Management Services Office in the Office of Management. It provides guidance for U.S. Department of Education (Department) employees' and contractors' use of Instant Messaging (IM) and Text Messaging (TM) communications tools on Department-owned technology or a Department-provided communications account.¹

The Department is working to gain a better understanding of IM and TM system capabilities in order to (1) evaluate how they improve Department Communications; and (2) determine how they can be incorporated into existing operations, while ensuring compliance with the Federal Records Act of 1950, as amended, and related records authorities (collectively, the Records Act). As explained in detail below, IM and TM tools are available to facilitate real-time communication about routine work activities, such as scheduling issues or clarifying work assignments, but are not intended to be used to conduct official Department business.

This joint guidance will remain in effect until the Department issues an ACS directive or other official policy governing the use of IM and TM communications tools.

II. SCOPE

This joint guidance applies to all IM and TM communications sent or received by Department employees or contractors using Department-owned technology or a Department-provided communications account.

IM is defined as an electronic messaging service that allows users to (1) determine whether a certain party is connected to the messaging system at the same time and (2) exchange messages with connected parties in real time. TM is defined as text messages between phones and fixed or portable devices over a network. In addition to sending text-based messages over IM and TM communications tools, users may have the ability to attach and exchange electronic files such as images, audio, video and documents. Communications exchanging electronic files are also covered by this guidance.

This joint guidance does not apply to email communications, paper documents, data releases and other forms of communication addressed by the policies and procedures in ACS Directive OM:6-103; or the Department's social media communications (e.g., Facebook), blog content, "tweets," etc. that are addressed by the policies and procedures in ACS Directive OCIO:3-109.

¹ The Department authorizes use of the following IM communication tools for the purposes specified in this document: Microsoft Communicator provided tools, including Office Communicator, Live Meeting and corresponding audio/visual communications capabilities. The Department authorizes use of the following TM communication tools, on a limited basis: SMS and Blackberry Messenger.

III. IM/TM USE LIMITATIONS

Users should not use IMs or TMs to conduct official Department business. Additionally, users should not use IMs or TMs for any inappropriate, unlawful, or otherwise abusive purpose.

The following is a non-exhaustive list of examples of **acceptable** IM or TM use that fall within the scope of the tools' intended use:

- Making routine requests for information, provided the request does not require administrative action, a policy decision, or any special compilation or research;
 - Checking a coworker's availability (e.g., 'Are you at your desk so that I come by and ask you a question?');
 - Asking a coworker to photocopy, scan or print documents; or
 - Asking a coworker if he or she has a file you need;
- Replying to routine requests, provided the reply does not require administrative action, a policy decision, or any special compilation or research;
- Asking a colleague to create a cover letter that does not add any information to the information contained in the materials being transmitted;
- Scheduling a meeting or a work-related trip or visit; and
- When "real time" interaction or clarification is needed on matters that do not concern the transaction of public business and do not concern a subject that would generate an official record;
 - Checking with a coworker to determine if she has made progress on a particular work assignment;
 - Suggesting an appropriate person to provide comments on a document.

The following is a non-exhaustive list of examples of **unacceptable** IM or TM use that fall outside the scope of the tools' intended use, which may inadvertently create an official record:

- Communications that generate an official record (this category includes, but is not limited to, communications that discuss a decision related to the substance of an ongoing project, or discuss different policy options);
- Holding meetings where official Department business is discussed;
- Discussing Department personnel issues, such as employee performance or discipline; and
- Discussing Department contracting issues, such as whether to sign a particular contract.

IV. RECORDS DEFINED

The criteria used by the Department to define "record" are outlined in ACS Directive OM:6-103.² Determining whether an IM or TM is a record depends on the content of the communication. An IM or TM that contains content consistent with the types of **acceptable** uses listed in Section III, above, has

² The Records Act defines "records" to include all "machine readable material," which is commonly interpreted to include electronic records stored on a computer "made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them." 44 U.S.C. 3301, as amended.

minimal documentary or evidential value and can be destroyed immediately.³ However, an IM or TM that contains content consistent with the types of communications listed as **unacceptable** uses in Section III, above, **may be a record**, and should be preserved according to the requirements of the Department's records management policy described in detail in ACS Directive OM:6-103.

V. RECORDS RETENTION

Employees and contractors should **not** use IM or TM systems to conduct official Department business as outlined in the above use examples. The Department recognizes, however, that Department employees and contractors use web conferencing and online collaboration tools (e.g., WebEx and LiveMeeting) to interact with the public. Using these tools saves travel costs and maximizes efficiency by allowing the Department to communicate with groups of interested parties at once from a central location. The communications tools used to interact with the public continue to evolve and add new technological capabilities, including IM and TM functions. If these tools are used to interact with the public and the substance of the communications meets the definition of a record, the employee or contractor using the tool is required to comply with applicable records retention requirements.

Whenever an IM or TM qualifies as a record, it is the individual IM or TM user's responsibility to preserve the communication. For assistance determining what communications qualify as records, and the appropriate method to store records, please contact the Department's Records Officer, Sherry Smith (Sherry.Smith@ed.gov). Also, ACS Directive OM:6-103 Records Information Management Program provides detailed instructions on how to preserve communications that qualify as records, and is found at: http://connected.ed.gov/document_handler.cfm?id=3548.

VI. NO EXPECTATION OF PRIVACY

Consistent with applicable Department policies and guidance, users have no expectation of privacy with regard to electronic messages, official or personal, sent or received through the Department-provided IM or TM communications services. At any time, the government may monitor, intercept, search and seize any communication or data transiting or stored on Department-provided information systems or communication services. For more guidance, please refer to the following policies: OCIO-1-104, Personal Use of Government Equipment and Information Resources, dated April 16, 2006; and OCIO-01, Handbook for Information Assurance Security Policy, dated December 19, 2005.

VII. CONCLUSION

This joint guidance seeks to allow the Department to explore ways to enhance and improve communications, while ensuring compliance with the Records Act.

³ See General Records Schedule 23, Transmittal No. 22 April 2010, Item 7.

Web 2.0 and Social Media Records Management Guidance

I: Purpose:

The purpose of this guidance is to provide records management requirements to Department of Education staff regarding compliance with the Department's records retention policies when using, managing, and maintaining Social Media/Web 2.0 technologies. Open and transparent government increasingly relies on the use of these technologies, and as agencies adopt these tools, they must comply with all records management laws, regulations, and policies. Successful compliance involves the active participation of agency records management staff, web managers, social media managers, information technology staff, privacy and information security staff, and other relevant stakeholders.

This document complements Departmental Directive 06-103, the Records and Information Management Program, and is applicable for all ED employees and contractor personnel using Web 2.0 technologies in an official capacity.

See also National Archives and Records Administration Bulletin 2011-02 and OMB M-10-23.

II. Background:

Web 2.0 and Social Media are terms that describe different web applications used for integrating web technology, social interaction, and user-generated content. Through social media, individuals or collaborations of individuals, create, organize, edit, comment on, combine, and share content. The Department endorses the use of social media and Web 2.0 tools and technologies to connect people to government and to share information (e.g., providing information or promoting discussion about ED, soliciting responses from the public, recruiting personnel, and providing collaborative space to work in new ways).

Web 2.0 and social media platforms can be used internally, externally, or both. In many instances these platforms are operated by nongovernmental third-party entities. Extra care must be taken when implementing Web 2.0 technologies or integrating these tools into the ED environment. Offices deploying Web 2.0 content must adhere to existing information assurance (IA) and privacy policy, guidance, and best practices.

Social Media/Web 2.0 platforms and technologies, include, but are not limited to:

Web Publishing: Platforms used to create, publish, and reuse content.

- Microblogging (Twitter, Plurk)
- Blogs (WordPress, Blogger)
- Wikis (Wikispaces, PBWiki)
- Mashups (Google Maps, popurls)

When agency content is duplicated across multiple platforms in an agency recordkeeping system, the agency may determine that the duplicate content is non-record. For example, if social media platforms are used to simply re-post news and other public affairs communication items that are captured and managed elsewhere, then the social media content may be considered non-record. Keep in mind, social media platforms may offer

better indexing, opportunity for public comment, or other collaboration. These factors may add value to the content making that content a record.

Social Networking: Platforms used to provide interactions and collaboration among users.

- Social Networking tools (Facebook, LinkedIn)
- Social Bookmarks (Delicious, Digg)
- Virtual Worlds (Second Life, OpenSim)
- Crowdsourcing/Social Voting (IdeaScale, Chaordix)

As agency records officers and social media managers consider what Web 2.0 content will be record material, they should identify which components or features of the content should be included. For example, an agency should evaluate which of the various components of a social networking profile, such as the profile itself, posts to the profile, and/or other interaction with the public should be retained as records.

File Sharing/Storage: Platforms used to share files and host content storage.

- Photo Libraries (Flickr, Picasa)
- Video Sharing (YouTube, Vimeo)
- Storage (Google Docs, Drop.io)
- Content Management (SharePoint, Drupal)

Any information stored or filed under such a system is subject to the Department's management if that information is a federal record. All record will be classified as part of a records series and the appropriate retention schedule will be applied.

III. Records Determination and Retention Policy:

ACS Directive OM 6-103 states that "[i]t is the policy of the Department to create, preserve, maintain, use, and dispose of Federal records in compliance with the requirements of the Federal Records Act and applicable NARA regulations, and to ensure access to information by Department officials, and the public, as appropriate." This includes Federal records created within Web 2.0 technologies and platforms.

NARA's guidance in Bulletin 2011-02 for determining record and non-record content provided on Web 2.0 and social media platforms is that the principles for analyzing, scheduling, and managing records are based on content and are independent of the medium. Where and how an agency creates, uses, or stores information does not affect how they identify Federal records. When using Web 2.0/social media platforms, the following non-exhaustive list of questions may help determine record status:

1. Is the information unique and not available anywhere else?
2. Does it contain evidence of an agency's policies, business, mission, etc.?
3. Is this tool being used in relation to the agency's work?
4. Is use of the tool authorized by the agency?
5. Is there a business need for the information?

If the answers to any of the above questions are yes, then the content is likely to be a Federal record.

Program Offices need to consider how frequently the information contained on various platforms will need to be captured. This determination is unique to each application and will depend on how frequently the content changes, the quantity of the content, the stability of the networking site, and the functionality of the tools available for extracting the information from the site. The PIRMS Records Management staff will assist the Program Offices in this assessment process.

IV. Roles and Responsibilities

Privacy Information and Records Management Services

The Department Records Officer shall:

1. Provide guidance and validate compliance with regards to Web 2.0 technologies related to records management and privacy issues.
2. Work with offices to determine whether content is a Federal record and provide guidance and instruction on securing and managing Federal records.

Principal Offices

Principal Offices shall:

1. Ensure that records created by their use of Web 2.0 technologies are captured and maintained in accordance with Departmental policy for records retention.
2. Confer with the Department Records Officer to apply existing disposition schedules to, or to schedule, official records created and/or maintained with social media and Web 2.0 platforms.
3. Ensure, in conjunction with the Office of the Chief Information Officer (OCIO), that appropriate management clauses for the retention of information hosted by a third-party provider are established, to include a Terms of Service agreement that ensures Departmental regulatory compliance.
4. Create content that will not pose a risk if it is available on the web indefinitely, because destroying it according to a records schedule may not be possible.

VI. Management and Retention of Web 2.0 and Social Media Information

Judging whether content posted on a social media site constitutes a record and is subject to traditional records retention and disposal practices is difficult. Principle Offices authorized to use Web 2.0 technologies should work closely with their Records Liaison Officers (RLOs) to determine what content constitutes a Federal record and to link these records to an appropriate records series to be managed under the retention schedule pursuant to the direction of the Department Records Officer.

