University of Chicago
Research Data Protection Policy

I. Introduction

The University, its faculty, and others engaged in research at the University have a common interest in ensuring that research data is managed in accordance with all applicable laws, regulations, contracts, University policies, and other requirements. In order to promote good research practices and mitigate the risks associated with improper treatment of research data, the University has adopted this Research Data Protection Policy (the "**Policy**").

II. Applicability of this Policy

This Policy applies to all University faculty, other academic appointees, employees, staff, postdoctoral fellows, students, and any other persons, including consultants, involved in the design, conduct, or reporting of research performed at, under the auspices of, or using the resources of the University.

III. Policy

All data and information held for research purposes must be managed in compliance with all laws, regulations, contracts, University policies, and other requirements.

IV. Research Data General Responsibilities

a. Principal Investigators are responsible for:

   i. ensuring compliance with this Policy for any data or information that they use in connection with their research;

   ii. being aware of any restrictions applicable to any data used in connection with their research and complying with those restrictions; and

   iii. consulting with University Research Administration (URA) for assistance identifying any restrictions on data used in connections with their research and ensuring that such data is managed in compliance with applicable laws, regulations, University policy, or contracts.

b. URA is responsible for, and has the sole authority for, approving and executing all contracts (each a "**Data Use Agreement**") on behalf of the University for:

   i. the receiving of data and information for research purposes; and

   ii. the sharing and transfer of data and information with third parties for research purposes.

c. URA's responsibility and authority for approving and executing Data Use Agreements includes Data Use Agreements with no monetary value.

d. URA may delegate its authority for Data Use Agreements to others within the University.

e. For avoidance of doubt, sharing or receiving data that is or can be made publicly available does not require a contract. If Principal Investigators choose to receive or share such data without a contract, they may do so without consulting with or approval from URA. URA's responsibility

for approving and executing contracts only applies when a contract is used for the exchange of data, regardless of whether the contract is required or optional.

f. The University Chief Information Security Officer (CISO) is responsible for approving information security measures implemented to protect the security of Restricted Data and aiding Principal Investigators and Information Technology personnel in implementing such measures. The University CISO may delegate the responsibility for approving information security measures to others within the University.

V. Restricted Data and Personally Identifiable Information

a. Principal Investigators are responsible for:

i. identifying any data they use in their research which is subject to restrictions set forth in any law, regulation, University policy, or contract ("**Restricted Data**") and understanding the applicable restrictions;

ii. consulting with URA to properly identify any Restricted Data and ensure that such Restricted Data is managed in compliance with applicable laws, regulations, University policy, or contracts;

iii. identifying and complying with the applicable restrictions on the processing, storage, use, access, or other utilization of Restricted Data for research;

iv. ensuring that all Restricted Data used or held for use for research purposes is stored on or accessed from University information technology resources in a manner approved by either: (1) the appropriate Institutional Review Board (IRB) in an approved research protocol; or (2) if an IRB protocol does not apply, the University Chief Information Security Officer (CISO);

v. ensuring that all Personally Identifiable Information used or held for use in their research is managed in a manner approved by either: (1) the appropriate IRB in an approved research protocol; or (2) if an IRB protocol does not apply, the responsible University privacy official; and

vi. identifying any unauthorized access to Restricted Data or disclosure of any Restricted Data or failure to comply with the terms and conditions of a Data Use Agreement and promptly reporting the data access, data disclosure, or agreement non-compliance to URA and, to the extent applicable, the IRB.

b. URA is responsible for assisting Principal Investigators in classifying research data, identifying any research data that is Restricted Data, and understanding any restrictions applicable thereto.

c. The University IRB's are responsible for approving the security measures implemented to protect Restricted Data used in human subject research as set forth in the applicable research protocol.

VI. Data Use Agreements

a. University Research Administration (URA) is responsible for confirming the following before executing a Data Use Agreement:

i. if Restricted Data will be transferred to the University, the University CISO (or his or her delegate) has approved a management plan;

ii. if Restricted Data will be transferred to outside organizations or individuals, such transfer is permitted under applicable laws, regulations, University policies and contracts;

iii. if Personally Identifiable Information will be transferred or received, the applicable privacy official and the appropriate IRB have approved of the research and any plan for ensuring the security of such Personally Identifiable Information; and

iv. the data is either: (1) not subject to any U.S. Export Control regulations; or (2) if the data is subject to U.S. Export Control regulations, that an appropriate plan is in place to ensure compliance with such regulations.

VII. Other Policies

Divisions, schools and departments may also adopt their own more stringent policies regarding protection of research data to supplement this Policy. If any such policy conflicts with this Policy, the terms of this Policy will apply.