Policy: Interim Privacy Policy for GDPR-Covered Data	**Policy No: I-7.7**
Policy Owner(s): Human Resources	**Original Date: 6/19/2018**
Last Revised Date	**Approved Date: 6/19/2018**

I. **POLICY**: It is the intent and stated practice of John Carroll University to create a framework to meet its compliance obligations for Data subject to the European Union's (EU) General Data Protection Regulation (GDPR). The University may be subject to the GDPR if it recruits students or employees in the EU, conducts marketing in the EU, participates in student or faculty exchange programs within the EU, conducts fundraising targeted to EU residents, conducts research with human subjects in the EU, or engages in other activities within the EU. The University will make its best efforts to modify its current Data handling practices to meet these new and developing legal obligations.

This interim policy describes the University's responsibility to implement additional privacy protections and procedures when collecting and processing Data concerning EU residents or gathering, storing, or processing Data in the EU. It also describes the Privacy Statements or policies adopted by different University divisions that are handling special categories of Data. All employees are expected to follow all applicable guidelines when handling Data covered by this policy in any form.

This is an interim policy and it will be updated as additional guidance is available and the University further develops internal Data handling practices.

II. **PURPOSE**: To ensure appropriate compliance with EU Data privacy regulations for covered Data.

III. **SCOPE**: All employees of John Carroll University or others acting on behalf of the University.

IV. **DEFINITIONS:**

GDPR: The European Union General Data Protection Regulation ("GDPR") became effective on May 25, 2018. Information concerning the GDPR can be found here: https://www.eugdpr.org/eugdpr.org.html.

Data: Personally identifiable information held by the University concerning any individual in any form, including both paper and electronic records. The GDPR defines personal Data to include any information related to an identified or identifiable person which may include but is not limited to a name, reference number, identification number, location Data, online identifier, email address, IP address, or one or more factors specific to a physical, physiological, genetic, mental, economic, cultural or social identity of a person.

Data Subject: A Data Subject is a person who can be identified, directly or indirectly, from information contained within Data. For the Purposes of this policy, Data Subject means a Data Subject that falls within the jurisdiction of the GDPR.

EU: The European Union. The EU is a political and legal association of countries consisting of the following members: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom[1].

V. POLICY ELABORATION:

A. Compliance Obligation: The GDPR is designed to protect the privacy of Data concerning EU residents, governs Data collected or processed in the EU or Data transferred out of the EU, and regulates entities that offer goods or services in the EU. This policy imposes additional requirements beyond the existing policies already in place under the University IT Resources Policy, FERPA obligations, and the Sensitive Data and Security Policy.

B. Data Processing: The GDPR requires personal Data to be processed lawfully, fairly and in a transparent manner, limited only to that Data which is necessary, maintained for accuracy, stored only for the length of time required or needed, and safeguarded from unauthorized disclosure.

C. Legal Basis for Data Use: Under the GDPR, JCU may collect and process personal Data for purposes including but not limited to the following:

1. The Data Subject has given consent to the processing for a specific purpose;
2. The processing is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract;
3. The processing is necessary for compliance with a legal obligation of the University;
4. The processing is necessary in order to protect the vital interests of the Data Subject or another person,
5. The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the University; or
6. The processing is necessary for the legitimate interests pursued by the University or by a third party, except where such interests are overridden by the interest of the fundamental rights and freedoms of the Data Subject which require protection of the personal Data.

D. Consent Forms: It is the policy of the University to have a Data Subject fill out a consent form when they start to provide JCU with a significant amount of Data,

[1]The UK will move into a different status if and when its exit from the EU concludes.

when it is required to establish a legal basis for collecting the Data under the GDPR, or when collecting sensitive Data about Data Subjects.

The University has developed the following consent forms for this purpose:

1. A consent template for use with Data Subjects is available and should be modified depending upon the nature of the use: http://webmedia.jcu.edu/global/files/2018/06/John-Carroll-University-GDPR-Consent-Form-rev.pdf . Consent to the collection and processing of personal Data must be explicit, and individuals must be provided the ability to revoke consent in as easy a manner as consent was given.

2. Consent for Advancement activities may be recorded by using the on-line form in the Interim University Advancement Privacy Policy at: http://sites.jcu.edu/advancement/advancement-privacy-policy/ .

E. **Privacy Notices**: Privacy Notices and/or policies have been adopted by certain University units to describe the personal Data collected, the applicable legal basis, the purposes for which Data is used, safeguards imposed, the retention period, and a point of contact for an individual to exercise rights under the GDPR. The University's Privacy Notices/policies can be found as follows:

1. Global Education: http://sites.jcu.edu/global/pages/global-education-privacy-statement/

2. University Advancement: http://sites.jcu.edu/hr/pages/resourcespolicies/technology-policies/

F. **Sensitive Data Protections**: The GDPR requires consent of the Data Subject, and the ability to revoke consent, whenever personal Data includes race, ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, genetic Data, biometric Data, health Data, sex life, or sexual orientation ("Sensitive Data"). For this category of Data, consent must be obtained unless an exception under the GDPR permits Sensitive Data to be collected and processed without consent.

G. **Reporting a Breach:** The GDPR includes a protocol for investigating, responding to and reporting the unauthorized disclosure of personal Data. Any employee who suspects a Data breach should promptly report it to the University Information Technology Services: http://sites.jcu.edu/its/pages/contact-us/, by emailing jspitz@jcu.edu, or calling 216-397-1614. The Help Desk will respond by following the University's processes for responding to a data breach.

H. **Exercising GDPR Rights**: Individuals who wish to exercise their rights under the GDPR should contact the email identified in the applicable Privacy Notice or Jamie Spitznagel, Data Security Engineer, at jspitz@jcu.edu or 216-397-1614. The University reserves the right to limit the Data impacted by such requests to Data that is within the jurisdiction of the GDPR.

I. **Data Protection Measures**: The GDPR requires the implementation of

appropriate Data protection measures taking into account the nature, scope, context and purposes of processing. Data protection should be intentional and should be a default assumption. The amount of Data held should be minimized; pseudonyms or de-identification should be used when aggregate Data is held and the identity of the individuals involved is unnecessary. Encryption should be used where appropriate. Data protection measures should take into consideration the risks presented by Data processing, accidental or unlawful destruction, loss, alteration, and unauthorized disclosure. If you have questions about Data protection measures, you should contact Jamie Spitznagel, Data Security Engineer, at jspitz@jcu.edu or 216-397-1614.

J. Third Party Data Handling: The University often uses third party systems to store and process personal Data. Third party providers must agree to safeguard University Data, which should be addressed during the contract review process. Departments should consult the Office of Legal Affairs for assistance with language for such third party contracts. Data also must be protected under the University's Sensitive Data Policy.

K. Data Retention: University departments are empowered to set their own appropriate Data retention policies. The GDPR requires the University to ensure that Data retention decisions are driven by operational need and do not result in the unnecessary retention of Data that is no longer needed.

L. Additional Information: Guidance issued by authorities within the EU to aid in the interpretation of the GDPR can be found here:

https://ec.europa.eu/info/law/law-topic/Data-protection_en.

M. Penalties: There are very significant financial consequences for a failure to abide by GDPR rules for covered entities. Financial penalties for non-compliance can be up to € 20 million Euros.

VI. CROSS REFERENCES:

I-7.1 IT Resources Policy

I-7.2 Sensitive Data and Security Policy