Administrative Guideline 1119

Adopted: June 26, 2018

ADMINISTRATIVE GUIDELINE TYPE: Information Technology

ADMINISTRATIVE GUIDELINE TITLE: General Data Privacy Regulation (GDPR)

DEPARTMENT RESPONSIBLE: Information Technology, International Services and all Employees

I. Statement of Purpose

The European Union (EU) General Data Protection Regulation (GDPR) enforcement becomes effective May 28, 2018. This regulation is designed to unify data privacy laws, to protect/empower all EU citizens (i.e. SCC international students) data privacy and to emphasize to organizations the importance of securing personal data.

Southeastern Community College (SCC) is committed to safeguarding the privacy of our students and personal data. This GDPR Administrative Guideline serves as the College's "Privacy Notice" for EU students and provides details on how SCC collects, processes, stores (hosts), and discloses personal data.

This guideline (Privacy Notice) will be administrated in accordance with SCC's comprehensive ITS security plan, which includes additional guidelines and procedures to ensure SCC protects the privacy of our students as well as comply with the EU's privacy regulation. SCC's security guidelines are referenced in Section XII.

II. Definitions and Terms

1. Data Processor - SCC will process personal data based on the student's consent to pursue educational/service opportunities at the College.
2. Data Controller - SCC will limit the data provided to third-party organizations based on the educational resources and services they are providing to students.
3. European Commission: GDPR Official Web Site
4. SCC's GDPR Privacy Policy - Administrative Guideline 1119
5. SEVIS - Student and Exchange Visitor Information System. SEVIS is a nation-wide information database system that maintains accurate and current information on International Students. The United States Department of Homeland Security requires all Colleges located in the United States to follow specific regulations, data collection and compliancy procedures.

III. Users Governed

This guideline applies to all SCC prospective and current students that are EU citizens as well as SCC employees (Information Technology (IT), International Programs, Athletics are focus areas). A hyperlink to a list of EU countries: List of Countries in the EU.

IV. GDPR Personal and Sensitive Data Definition

The European Commission (documented in their GPDR regulation document) defines personal data as "any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data."

In addition, the European Commission defines sensitive personal data as consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

Personal/Sensitive data examples include:

1. a name, date of birth, address, telephone number and email address
2. an identification card number
3. location data (for example the location data function on a mobile phone)

4. racial or ethnic origin
5. gender or sexual orientation
6. health or medical information
7. online identifier (i.e. IP Addresses, Device ID)
8. Web site or electronic collection of data through a technical system (i.e. cookie ID)

Southeastern Community College will minimize the collection of personal data to information that is required to process an EU students' legitimate interest or is legally/regulatory required as part of state/federal regulations.

V. Data Collection

SCC collects, processes, stores and discloses personal data as required to meet the educational objectives of each student, provide a safe environment and to comply with state/federal requirements. Based on SCC's human resource procedures and security controls, data should only be collected by authorized personnel who have passed background checks, have job responsibilities specific to the information collected and participate in annual training on the importance of securing personal data.

Information collected for educational interests and state/federal regulations include:

1. Recruiting Initiatives and Information Request by Student
2. Application and Enrollment Data
3. Academic Advising
4. Academic Program Requirements
5. Student Account Information - to access computer and online resources
6. Student and Exchange Visitor Information System (SEVIS) - required by United States Department of Homeland Security
7. Accreditation - required by Higher Learning Commission
8. Emergency Contact Information - student safety
9. State and Federal Reporting
10. Internal Analysis - to improve academic programs and international program/services
11. Athletics, Clubs, Activities and College-Sponsored Initiatives - Collection of data related to this category will be based on the voluntary actions of the EU student wishing to participate.
12. Other Related Processes

VI. Website and Electronic Technical Collection of Personal Data

SCC may use cookies/tracking/logging strategies to enhance the user experience, collect information to improve site navigation strategies and to improve system performance. Users may turn off their browser's "cookie" feature by accessing the settings and completing the necessary steps.

VII. Web Forms

SCC has electronic forms on the College's Web site that requests personal data from prospective students in order to process legitimate interests such as requesting additional information, applying, registration, etc. These forms are designed to provide students with efficient methods to process their educational aspirations. Please note by accessing and using these resources, students are consenting to having their data collected and processed at SCC.

VIII. Consent for Data Collection

SCC's International Program Office will provide an electronic copy of this guideline to all prospective students with EU citizenship that have communicated an interest in attending the College. After reviewing this guideline in detail, the student will be asked to sign the "GDPR Consent Agreement Form" at the bottom of this document. By reading and signing the consent agreement, the student confirms their understanding of SCC's GDPR Guideline (Administrative Guideline 1119).

IX. Data Storage (Hosted)

The personal data provided by students during the application, registration and service processes is stored in a secure database accessible by the College's "Student Information System" (SIS). Data needed for reporting and regulatory requirements is stored in a secure network location. In addition, physical documents are stored in a secure environment. SCC has implemented a comprehensive set of technical and physical safeguards to protect personal data and only allow authorized personnel to have access to this information.

Third party organizations, that partner with SCC, may store limited personal data based on the specific needs of the students related to the systems and services that are provided.

X. Third Party Disclosure of Confidential Data

Disclosure of personal data to third party organizations will be based on the educational and service needs of each student.

Personal data may be disclosed to third-party organizations for the following purposes:

1. Consent - the student requests and gives permission to disclose information on their behalf. This process is initiated and documented through the Data Protection Officer. Contact information for the Data Protection Officer is located in Section XI.
2. Regulatory - SCC is required to provide student information to comply with state/federal regulations and reporting requirements. Only information that is required by these agencies will be provided.
3. Legal Obligation - Student information may be shared as required by local, state and federal laws.
4. Public Information - SCC will only share your information to the "Public" if a student voluntarily participates in athletics, clubs, activities or other College-sponsored initiatives. For example, if a student participates on the College's volleyball team, the student's personal data (example: name, height, country) may be on the Iowa Community College Athletic Web site, in the local newspapers and other public resources.
5. Educational Systems - Student information may be shared with third party resources such as the Canvas Learning Management System (LMS), Publishers Learning Environments and other services related to the students' specific educational pathway. For example, students will need to access the Canvas LMS to access online course(s), academic program content, digital media, etc.
6. College Partnerships - personal data may be shared with organizations/companies that are affiliated with the College to meet the educational or service needs of the students. This data will only be shared based on the services and systems needed by each individual student. For example, SCC partners with a company to provide on-site student housing. Personal data will be shared with this company in order to provide secure access, housing services and emergency contact/support. Examples of additional College partners are provided below:
    A. Student Housing
    B. Food Service
    C. National Clearinghouse - Transcripts (Academic Records)
    D. Community Service Providers
    E. Technology Service Providers

XI. Rights of GDPR Data Subjects

The table below provides a list of EU student rights along with SCC's compliancy strategies:

GDPR Subject Right	SCC Strategy
Privacy Policy	This guideline (Administrative Guideline 1119) serves as the "GDPR Privacy Policy".
Data Protection Officer	Chuck Chrisman, Executive Director of Technology Services has been designated as the Data Protection Officer. Chuck can be contacted by: phone: 1-319-208-5070 email: cchrisman@scciowa.edu address: 1500 W. Agency Road, West Burlington, Iowa 52655

Data Minimization	SCC will only collect personal data that is required to meet the student's educational/service needs, provide a safe environment and to comply with state/federal requirements
Access to Data	Students can securely access some personal data/ information on the https://scciowa.sharepoint.com/sites/hawknet Web site. Data requests can also be made through the Data Protection Officer.
Data Rectification	SCC will correct any incorrect information as soon as it is verified. Students can contact the Data Protection Officer to initiate and process the data rectification request.
Right to Erasure	Data that is collected for educational programs, legal or regulatory requirements will not be destroyed (erased) and considered part of the student's "Permanent Record". As documented throughout this guideline, the data will be securely stored and only accessible by authorized personnel. Data that is not required for educational programs, legal or regulatory requirements will be erased upon request. Written requests should be made through the Data Protection Officer.
Data Portability	SCC will only transfer personal data to meet the specific educational/service needs of EU students. This is described above in Section X.
Data Breach	Data Security Officer will notify EU Commission GDPR authorities within 72 hours of a known data breach. In addition, the Data Security Officer will notify students' that are impacted by a data breach according to the College's Administrative Guideline 1116, "Employee Guidelines for Reporting Security Incidents".
GDPR Requests, Questions, Concerns	Please contact Chuck Chrisman with any GDPR requests, questions and concerns. Contact information listed above.

XII. References

1. Administrative Guideline 306 - Procedures for Meeting the Family Educational Rights and Privacy Act (FERPA)
2. Administrative Guideline 1111 - Ellucian Security Access
3. Administrative Guideline 1114 - Employee Guidelines for Securing Confidential Data
4. Administrative Guideline 1116 - Employee Guidelines for Reporting Security Incidents

XIII.

Please review and complete section XIII, the GPDR Consent Agreement Form.