Meta Data TBD

DRAFT - Privacy Policies

V. Background

The Cooper Union is committed to protecting the privacy and confidentiality of the personal information provided by students, faculty, staff, and research partners. The school has established policies, standards, and practices to protect personal information in accordance with applicable privacy and data protection laws and regulations. These regulations include federal, local, and international laws including the Family Educational Rights and Privacy Act (FERPA), General Data Protection Regulations (GDPR) and the Gramm Leach-Bliley Act (GLBA). Every member of the Cooper Union community is responsible for upholding the data standards and provisions established by these regulations. Faculty and staff are responsible for adhering to practices that protect the privacy and confidentiality of student data, records, and disclosures, and the security of the data and education records maintained by Cooper Union. The Privacy policy provides an overview of data governance that supports the privacy and security provisions established in FERPA, GDPR, and GLBA.

Deleted:

VI. Rationale

Student information stored in all forms including paper and electronic format, must be secure and available only to those entitled to access that information. Because data sharing is facilitated by the digitization of information and prevalence of electronic mediums, information technology plays a crucial role in establishing electronic protections to support key privacy principles. Faculty and staff accessing and storing confidential information in unsecure locations (e.g., flash drives, public or home computers, etc.) creates the risk of unauthorized access to protected education records. For this reason, there are strict guidelines as to how staff and faculty communicate on records, and the systems used for communication particularly to protect the student record and confidential transactions with students. Federal regulations not only stipulate controls for the protection of information, but they may also require the ability to remove records as is the case in provisions of the General Data Protection Regulations (GDPR) and to address security breaches. Engaging in unsecure and ubiquitous systems therefore introduces risks to Cooper Union's compliance with federal regulations and is therefore strictly monitored and prohibited.

The curation and use of data is essential to Cooper Union's academic, administrative and research operations. Governance and oversight practices are put in place to ensure that the school maintains the highest standards in the collection, storage, and use of personal information, including fair information principles that provide for notice, choices regarding information sharing and consent, the ability to access and alter data, accuracy and security of data, and mechanisms to enforce data and address breaches. Cooper Union's privacy policy discloses the privacy standards and practices upheld by the various academic and administrative units to mitigate threats such as identity theft, improper access, and unauthorized disclosures; and specifically addresses the controls put in place by information systems'<LINK> governance to provide needed transparency and protections.

Commented [AT1]: Brian Cusack- databases and roles; who has access

Commented [AT2]: Hyperlink IT to Data Privacy Policy

Student, Faculty and Staff records are considered confidential and may not be released without their written consent unless there is a legal,

A. Definitions

- **Privacy:** is an individual's right to be free from intrusion into their personal information. Privacy and data protection laws protect one's right to control how information about them is accessed, used, or shared. However, there are limitations to privacy rights; some information must be shared to provide students, faculty, and staff with a service or to perform certain administrative functions. For example, this is particularly true for the flow of information between key academic and administrative offices to support students. A student's information may be used without their express permission to register course grades. Although there are strong feelings about what information can be shared, there are critical concepts like Need to Know that will govern who has access to records and with whom those records can be shared. It is important to remember that students, faculty, and staff will have some control over who has access to their information and records.
- **Confidentiality: Except directory information, all student records are considered confidential and may not be released.** Individuals may request to suppress their information using the Request to Withhold Directory Information available through the office of the Registrar. Moreover, Confidentiality refers to how identifiable data is treated. Faculty and staff are ethically obliged, to the extent possible, to protect data that was shared in confidence against unauthorized uses or disclosures. Although privacy and confidentiality are used interchangeably, privacy is about an individual's rights to restrict access to their information; confidentiality is an ethical obligation on the part of the recipient of one's' data to protect the information and data they have been provided.
- **Data subscribers:** those Cooper Union entities that have been vetted by the office of Information Technology and granted data access. This is a broad term to describe anyone with access to data. Data subscribers are accountable to adhere to the guidelines that assure the privacy and integrity of data.
- **Directory and Public Information**: This is "...information contained in an education record of a student which would not generally be considered harmful or an invasion of privacy if disclosed" (FERPA Regulations, 34CFR, Part 99.3). Cooper Union's determination of directory information is established in the FERPA policy.
- **Education Record:** Education records are related to a student and are maintained by an educational agency or institution or a party acting for or on behalf of the agency or institution. These records include but are not limited to: Grades, transcripts, class lists, course schedules, financial information, and discipline files. The information may be recorded in any medium (e.g., print, handwritten, email, video, or audio tape, etc.). Exempted from the definition of education records are sole possession records/notes. Sharing or placing the records in an area where they can be viewed by others makes them subject to FERPA.
- **Need to Know:** is a basic principle put in place to protect student data. FERPA permits an educational agency or institution to disclose, without consent, personally identifiable information from students' education records only to school officials within the educational agency or institution that the educational agency or institution has determined to have legitimate educational interests in the information, aka Need

to Know. A school official has a legitimate educational interest if they need to review an education record to fulfill their professional responsibility.

Student information stored in electronic format must be secure and available only to those entitled to access that information. Faculty and staff have a legal responsibility under FERPA to protect the confidentiality of student education records in their possession. Access to student information is only for legitimate use in completing their university employee responsibilities. Access to student information, including online directory and public information, is based on one's faculty or staff role within the university. Faculty and staff may not release lists or files with student information to any third party outside their college or departmental unit. The provisions under FERPA are essential to also supporting the regulations established in GDPR and GLBA.

- **Multi-factor authentication (MFA):** is a mandate for Cooper Union to carry cyber insurance and comply with numerous regulatory requirements. Implementation of MFA started in December 2021. Educational institutions face a wide range of digital and physical threats, ranging from targeted violence to cyberattacks. Multifactor authentication is a layered approach to securing data and applications and thereby mitigate cyber threats. MFA is a system that requires a user to present a combination of two or more credentials to verify their identity for login and access to data. MFA increases security because even if one credential becomes compromised, unauthorized users will be unable to meet the second authentication requirement and will not be able to access the targeted computing device, network, or database. MFA supports Cooper Union's ability to mitigate Cybersecurity Scenarios which include cyber threat vector topics such as ransomware, insider threats, and phishing.
- **Personal Data: information relating to an identified or identifiable individual; an identifiable individual can be identified, directly or indirectly, by using any identifier or characteristic specific to that individual.**
- **Relevant Law**: any non-U.S. authority's personal data protection law that applies to the processing of Personal Data by a Cooper Union
- **Relevant Country**: a country which has enacted a Relevant Law.
- **In-scope Processing**: the collection, use, handling, processing, or sharing of Personal Data by a Cooper Union entity when those activities are within the scope of any Relevant Law.
- **Cooper Union Entity**: faculty, staff, students, or stakeholders acting on behalf of the institution.

B. Principles

Cooper Union strives to provide information to data subjects on several key elements relating to the processing of their personal data. Privacy practices are rooted in the following principles:

- **The Notice Principle:** Notice refers to the fact that the person providing information must be made aware of exactly who the information is going to and what it will be used for. Also referred to as transparency, this is of the utmost importance so that the consumer is well-equipped to decide about whether to hand over information, as well as which information they want to divulge. Information can

include the type of data collected, purpose of processing, right of access and choice, conditions for onward transfers and liability.

- **The Data Integrity and Purpose Limitation Principle:** Cooper Union strives to limit personal data to what is relevant for the purpose of processing, reliable for its intended use, accurate, complete, and current. Where a new (changed) purpose is materially different but still compatible with the original purpose, the Choice Principle gives data subjects the right to object (i.e., opt out). Specific purposes under this principle include archiving in the public interest, journalism, literature and art, scientific and historical research, and statistical analysis (fair use).
- **The Access Principle:** data subjects have the right to obtain from an organization whether such organization is processing personal data related to them. Data subjects must be able to correct, amend or delete personal information where it is inaccurate or has been processed in violation of the principles.
- **The Security Principle:** organizations creating, maintaining, using, or disseminating personal data must take "reasonable and appropriate" security measures, considering the risks involved in the processing and the nature of the data.

III. Privacy Policy

The collection and use of data are integral to Cooper Union's ability to achieve its mission. Several types and forms of data are collected by data owners across The Cooper Union to support daily operations and reporting obligations. The Privacy Policy establishes the regulations that govern Cooper Union's requirements, standards, and guidelines regarding the treatment of information and data protections to shield personal information and support compliance with federal, state, and international regulations.

Cooper Union complies with several laws to protect the privacy of the personal information contained in the various databases used by Cooper Union. These regulations include:

- The Family Educational Rights and Privacy Act, FERPA <LINK>
- Payment Card Industry Standards < https://www.pcisecuritystandards.org/document_library/>
- Gramm Leach Bliley Act, GLBA < https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act>
- The New York Shield Act < https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/new-york-shield-act.html>

Each regulation is addressed separately in this policy, showing the application of the key principles that guide how Cooper Union engages with data to protect student, faculty, and staff records and data. Importantly, this policy establishes the critical role that the Information Technology (IT) office plays in implementing a privacy plan that complies with regulations and fosters accountability to key privacy principles across the institution. IT provides oversight for Cooper Union's information privacy and data protection efforts where the Schools, Faculty of HSS, and administrative units are responsible to engage in the principles and practices that support data privacy and security.

The office of Information Technology establishes the practices that assure the privacy of education and financial records and puts in place the controls that will promote an environment that is ethical, accountable, and secure. All systems, computing services and security updates are centrally managed, supporting the ability of Cooper Union to comply with privacy and security regulations, and to address any breach of privacy.

Data Governance

Commented [AT3]: This should be a separate policy

Data is managed as an asset that supports the Cooper Union mission. The Information Technology office has established data governance protocols with the goals of ensuring that data provides value in that it is accurate and that processes established in the handling of data and the education records meets regulatory requirements including that risks are managed appropriately. Because poor handling of data poses a risk to the Cooper Union operations and planning as well as the sanctity of the education record, it is necessary to define roles and responsibilities for the management of certain types of data. Federal and state regulations exist to protect records and data, whether it is stored at Cooper Union or on a third-party system.

Definitions specific to Data Governance

At Cooper Union:

- **Data stewards** are accountable for managing, protecting, and ensuring the integrity and usefulness of Cooper Union data. Data stewards are principally responsible for ensuring that Cooper Union is following its policies and complies with federal and state laws and regulations. The Information Technology office is responsible for the stewardship of data.
- **Data custodians** have control over the disposition of data records, whether they are being created, stored, or are in transit between systems. Custodians will often have modification or distribution privileges meaning they often provide data to users. They carry responsibility to protect data and prevent unauthorized use. These functions are assumed by IT.
- **Data owners** have decision making responsibilities. They participate in processes to establish the contexts and definitions for data elements. The data owners are among senior administrators with unit level oversight. Definitions are established by regulatory and reporting agencies, so data owners are responsible for maintaining data definitions and assuring reporting compliance.
- **Data Users** create Cooper Union records and / or data; control the disposition of the data; and are responsible as custodians of the data. They support data custodians and owners in managing and protecting data by understanding and following information security policies and practices related to data use, especially in the practices that support privacy of the education record vis a vis, transmittal practices.
- **Data breach** is a security violation in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, altered, or used by an individual unauthorized to do so.
- **Personal Data** refers to any information that relates to an identified or identifiable natural person (i.e., an individual, not a company or other legal entity), otherwise known as a "data subject."

When Cooper Union units (owners and users) create shared data repositories they take on responsibilities as data custodians. They are responsible for working with data stewards to ensure that they understand Cooper Union's data management requirements and regulatory obligations. They may not extend the use of university data beyond the initial scope without additional review by the appropriate data steward, generally IT.

When shared data repositories are created on third party services, exceptional care must be made to ensure that contracts or service agreements include appropriate security and privacy provisions. The Information Technology and Controllers' offices at Cooper Union support compliance with this requirement.

"Need to Know" is a principle that governs how the Information Technology office (IT) provides access to student, faculty, and staff records. Several records exist for students, faculty, alumni, and staff across the data systems (academic, financial, alumni and human resource systems). Only those with legitimate educational interests (the "need to know") have access to record level data with access to specific records being strictly controlled by IT. "Need to know" is determined by the senior administrator of each data area and executed by giving a set of permissions (security classes) to those identified as having the need to access certain records, a "verifiable need to know". (This is especially pertinent to the education record which is strictly governed by FERPA and GDPR regulations.)

Appropriate permissions are discussed with each senior administrator and applied by IT. The complete set of permissions for all users are audited and reviewed annually by IT with each senior administrator being responsible to determine that 1) their direct reports have appropriate permissions to execute their job functions and 2) anyone outside their area with access permissions to records in their area have legitimate need as established in their scope of work.

- Access to the data system and records is approved by the hiring manager (data owner) and controlled by IT (data steward and custodian). Should a Cooper Union entity seek access, they should first seek approval from their manager.
- Data is verified by the senior administrator team responsible for the data, the "data owner." To mitigate unintentional disclosures and breaches of privacy, data files secured from data owners should not be shared across other units. Unauthorized sharing of student, faculty or staff level data or records is considered a data breach and may require the intervention of the IT team. Data sharing oversight is provided by data steward/custodians.
- An annual audit is conducted by IT to verify that the security classes assigned to data custodians and subscribers are appropriate.
- Roles and responsibilities of data owners and users necessitate a VPN connection with multi-factor authentication. A Virtual Private Network (VPN) enabled through IT creates a secure connection to the Cooper Union network for access to sensitive tools and resources such as data. A VPN protects users by encrypting their data and masking their IP address, leaving their browsing history and location untraceable. This greater anonymity allows for greater privacy, especially when working remotely.
- All data subscribers must comply with data standards. Because data subscribers do not have granting authority – they cannot assign permissions—they must not share the student level data provided them.

The Chief Information Technology Officer (CIO) shall maintain and publish a list of identified data stewards, custodians and owners for specific education records and data types. The list will also identify the classification of specific data types. Where a single individual maintains multiple roles (e.g., data steward and data custodian) the CTO will assess to ensure these roles do not pose a risk to The Cooper Union.

Additional details can be found in Cooper Union's Data Governance plan.

Data Security

A data breach is a security violation in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, altered, or used by an individual unauthorized to do so. To protect data and mitigate the occurrence of any breach of privacy, faculty and staff are required to only use software platforms approved by IT. Platforms include MS Outlook and Outlook Suite and MS Teams. Because these platforms require multi-factor authentication and are centrally managed by IT, Cooper Union can contain any breach or security risk.

- Faculty, staff, and students' exchanges must be conducted using approved communication channels like Microsoft Outlook or Teams©. These software tools require authentication and establish a contained environment over which IT has oversight. This capability is critical in supporting the privacy and security plan.
- Authentication and guidance regarding the access to, and transmittal of data support information privacy. Moreover, the fact of a contained environment supports the ability to remove records should it be required, further supporting specific privacy regulations. The General Data Protection Regulations (GDPR) requires this ability to remove or "disable" records. Once records are shared outside the Microsoft environment, for instance through Gmail transmittal, Cooper Union can neither assure the privacy or security of the records and loses the ability to disable all records. Furthermore, this has implications for Cooper Union's response to a data breach. Therefore, the use of Gmail to correspond on Cooper Union academic and administrative business, or to correspond in a professional, role specific capacity, is strictly prohibited.
- The onboarding process for new hires includes technology preferences, an inventory of the software applications provided by Cooper Union, and a request to enumerate additional software application preferences. Requests for additional software requests are vetted by the office of Information Technology to assure regulatory compliance and security. Therefore, approval is required for additional software requests and purchases.
- Faculty requests for new software can be made each term using the Acceptable Use Technology Request Form (hyperlink to the form). This form is to be used to request new software and ensure that the proposed software is compliant with privacy and security regulations and within the scope of the privacy and security plan requirements. Therefore, approval is required for additional software requests and purchases.

Commented [AT4]: This should be in a separate policy , information technology security

- Student records are purged from **Teams and Moodle** annually at the end of the school year in compliance with privacy requirements established in the Family Educational Rights and Privacy Act, FERPA. All class records and recordings are purged and moved to a SharePoint site where they are archived (attendance and course engagement are considered elements of the education record). SharePoint exists within the Microsoft environment and requires authentication.

The standards of operations established by IT facilitate Cooper Union's ability to disable/ and or remove student records in accordance with provisions established in GDPR.

There are three overarching Privacy Policies that govern the data protocols and management at Cooper Union:

- The **Family Educational Rights and Privacy Act, FERPA**
- The **General Data Protection Regulations (GDPR)**
- The **Gramm Leach Bliley Act, GLBA**
- The **New York Shield Act**

The principles underlying these policies drive critical data privacy, security and data management protocols that govern the access, processing, use and sharing of data.

Privacy Committee

Cooper Union will convene a Data Privacy Committee to oversee the appropriate oversight policies necessary to ensure that the highest ethical standards are maintained in the storage, collection, and use of personal data, that issues of bias and consent associated with data analysis are carefully weighed and that compliance with relevant international, federal, and state laws is maintained. The Privacy Committee will comprise senior leaders, the data stewards, and owners, from academic and administrative units. The Committee will be under the authority of the Vice President of Academic Affairs and the Chief Technology Officer, CTO. The committee will meet twice per term. The Committee will

- Develop a statement of principle and guidelines for deciding about specific data access and use proposals for data use.
- Build institution-wide understanding of the community's responsibility in protecting privacy and promoting data security.
- Review the privacy statements and recommend changes, as appropriate.
- Review privacy and security policies and weigh the protection of private and confidential data against Cooper Union's legal obligations as needed.
- Stay apprised of rapidly changing privacy laws and offer insights to Cooper Union's Cabinet on how to navigate the regulatory environment.
- Determine and act on areas of Privacy and Security that rise to the level of the Committe
- Act on behalf of the VPAA and VP Finance upon request

IV. Specific Privacy Policies

1. FERPA Privacy Policy

FERPA is short for the Family Educational Rights and Privacy Act, a federal law enacted in 1974. FERPA protects the privacy of student education records. All educational institutions that receive federal funding, including Cooper Union, must comply with FERPA. FERPA begins for students on the first day of classes/semester or attendance, whichever comes first, and the student continues to be protected by FERPA for their lifetime.

The full policy can be found at <LINK>

Commented [AT5]: Template providing needed statements provided to Mark Campell

2. General Data Protection Regulations (GDPR): Privacy Disclosures Under Non-US Law for Individuals Located Outside of the United States

Commented [AT6]: This should be a webpage, with policy link as with FERPA

GDPR, effective as of May 25, 2018, is a far-reaching regulation applicable to organizations with European Economic Area ("EEA") based operations and certain non-EEA organizations that process the Personal Data of individuals in the EEA. For purposes of GDPR, Personal Data refers to any information that relates to an identified or identifiable natural person (i.e., an individual, not a company or other legal entity), otherwise known as a "data subject." GDPR established data protocols assure privacy and security.

Rationale:

Technology – and the internet – have become ubiquitous, so much so that data standards are needed to protect an individual's personal data and privacy. In higher education, academic and administrative operational/in-scope processing relies on software systems, databases, and data sharing to support the ability to deliver mission driven and educational priorities. Whereas data protocols, security and data management are best practices that assure the protection of data, as they relate to personal data, they are fundamental to assure an individual's privacy. Privacy has been established as a fundamental human right as part of the European Union Convention on Human Rights, resulting in practices and regulations ensuring privacy protection through guiding regulations.

This policy provides disclosures that demonstrate Cooper Union's compliance with the European Union's General Data Protection Regulations and sets forth practices that support Cooper Union's adherence to privacy and security principles.

For the purposes of this policy:

- GDPR means the European Union's General Data Processing Regulation;
- With respect to individuals in the U.K., references to "GDPR" should be read as referring to the U.K.'s similar legislation, "the Data Protection Act of 2018";
- "Personal data" means information relating to an identified or identifiable individual who can be identified, directly or indirectly, by use of any identifier or factor specific to that individual; and

- GDPR "processing activities" means the collection, use, processing or sharing of personal data when those activities are within the scope of GDPR.

- Cooper Union collects personal information that is voluntarily submitted through online applications, surveys, and other contact and submission forms. This information may include a student's name, address, telephone numbers, e-mail, student ID, and password. Depending on one's role at Cooper Union, information is collected based on the requirements of the program, administrative or academic service, or engagement to support in scope processing activities. Please refer to the Cooper Union Privacy policy for detail. All information is collected in accordance with established regulations and security protocols, establishing that:
- Access to and Use of Personal data maintained in the data system is role specific; student level data should be maintained by role specific data managers and shared only on the basis of "need to know."
- Data protocols are established to prevent untoward access to the personal information of students, faculty, and staff and mitigate the potential of data breaches.
- To this end, information systems and software are vetted by the Chief Technology Officer for use by the Cooper Union community to support key academic and administrative functions while addressing risks for data breaches. The Cooper Union community is required to use the approved systems.
- The Information Technology office has specified information and software systems and practices that support privacy and security. Only the identified systems can be used in managing private and confidential academic and administrative records.
- By adhering to the use of approved systems, faculty and staff support data security and privacy. Adherence to GDPR requires the ability of the Information Technology office to remove records. Maintaining data and information exchanges in a closed system will support this ability and agile response to security threats.
- New software or apps requests should be advanced to IT for review and approval. This is a security measure to protect the privacy of records.
- Data and information purposes are specified and limited.

Cooper Union and third parties use personal data for the primary purposes of conducting analysis, responding to requests, and providing students with relevant information including program offerings that we believe may be of interest.

Key Definitions in GDPR:

- **Personal data** — Personal data is any information that relates to an individual who can be directly or indirectly identified. Names and email addresses are obviously personal data. Location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions can also be personal data. **Pseudonymous** data can also fall under the definition if it is easy to ID someone from it.
- **Data processing** — Any action performed on data, whether automated or manual. Examples include collecting, recording, organizing, structuring, storing, using, erasing data/

- **Data subject** — The person whose data is processed. These include students, faculty, staff or even website site visitors.
- **Data controller** — The person who decides why and how personal data will be processed. At Cooper Union, the Information Technology office establishes data controllers for the various academic and administrative units to assure data integrity and accountability to data privacy, security, and management.

Commented [AT7]: Or is this the CTO

This policy is broken out into sections:

- **PART A to Address:**
  - **The Notice Principle:** Who the information is going to and what it will be used for.
  - **The Data Integrity and Purpose Limitation Principle:** Provide assurance that personal data collected is limited to what is relevant for the purpose of processing, reliable for its intended use, accurate, complete, and current. This means that Cooper Union will collect and process only as much data as specified by the purpose. To support Data Integrity, Cooper Union will keep personal data accurate and up to date.

- **PART B to Address:**
  - **The Access Principle:** Establish that Cooper Union is processing personal data related to faculty, staff, and students. Data is broken out by "administrative"/ "academic" purpose to facilitate the ability to correct, amend or delete personal information where it is inaccurate or has been processed in violation of the principles. Rights regarding one's record are explicated in "Rights You May Have."
  - **The Security Principle:** Measures to protect data – data management, data transfer, and data retention practices are established. Data will only be stored as long as necessary for the specified purpose.

- **PART A:**

Notice of Types of Information Collected and Data Integrity and Purpose by Administrative Function

In this section, we establish the administrative units / functions that collect Personal Data, specify the data collected and establish the purpose and use of the Personal Data collected. The administrative units/functions include:

A. Admission and Financial Aid
B. Alumni and Donors
C. Online Functionality and Supports
D. In person engagement in Foreign Countries
E. Research
F. Employment
G. Third Party Providers
H. Other Uses of Personal Data

A.1 Admission and Financial Aid

Commented [AT8]: Mark to review and refine

Cooper Union collects and uses various kinds of Personal Data when a student applies for admission to a Cooper Union School or to a program or course offered by us, and when applying for financial aid. The primary source of these data is the student's voluntary submissions through applications, forms, etc. Cooper Union may solicit additional information from other available sources when looking for potential candidates for admission in connection with recruiting activities. The Personal Data collected by Cooper Union during the admissions process is used for the primary purposes of considering an applicant's candidacy for admission to the relevant school, program or course, evaluating a student's eligibility for financial aid, if applicable, and, if admitted and enrolled, facilitating the student's education (such as by sharing Personal Data with registrars and others in order to enable enrollment and participation in the school, program or course to which the student has been admitted). Third-party vendors include application and admissions/financial aid database vendors such as the Common Application, the College Board.

A.2 Personal Data Collected in conjunction with Admission Records include:

- **Contact Information:** Name, address, country, province, phone number, email address, emergency contact information. Outreach is conducted to maintain current information.
- **Academic Information Collected:** High school attended (HS), HS address, HS GPA, Test Scores: SAT, ACT, TOEFL, IELTS, AP/IB scores, summer college and GPA, previous college names, degrees, GPAs, current college, current class (Freshman – Senior), degree program, course grades, financial aid, student accounts data, and family and significant other educational background.
- **Citizenship status**: visa information (visa documentation is maintained in a restricted database) with residency and statement of status, and international address maintained in institutional database.
- **Engagement information:** Visit attendance, organization and precollege affiliations, competitions, awards, and honors.
- **Medical / accommodation** information may be discussed in essays.
- **Employment Information:** Company name, address, phone, email, position description, position/title, years in job, responsibilities, next step in career path, resume (upload).
- **Financial Information:** for example, government identification number, personal and business tax reports, wage reports and statements, bank statements, socioeconomic status, scholarships and grants, and family support. This includes FAFSA information, New York aid - TAP, external awards, citizenship status.
- **Family Information**: including family member names, ages, education information, occupations, wages, and savings;
- **Payment Information**: depending on a student's means of payment and/or refund including payment card number or bank and bank account number;
- **Log Files, Cookies, Location Information, and Mobile Device Sensor Information**: When one uses Cooper websites or mobile applications, Cooper may collect additional information as described in the Website engagement section.
- **Prospective student**'s behavior is tracked through our Slate communications (whether an email was opened or not, what links if any were clicked, browser location, device type, and if they traveled to any Cooper webpages and the time spent on those webpages).

- **Virtual tour visitor** behavior is tracked to aid us in optimizing the experience for visitors.

A.3 The Purpose of Collecting this Information:

Cooper Union collects this data as part of the admission and financial aid processing to

- Consider candidacy for admission and eligibility for financial aid;
- Respond to requests and communicate admissions and financial aid decisions;
- Facilitate operations relating to the admissions and financial aid process;
- Conduct research and analytics (for example, relating to application and admissions trends; and to support compliance reporting);
- Provide information and services related to the course or program, including assistance with residential and medical needs;
- Satisfy legal, regulatory, and contractual obligations; or
- Engage in other activities described under "Additional Uses of Personal Data."

Cooper Union processes Personal Data for the purposes described below consistent with the legal bases recognized by the Relevant Law in each Relevant Country. This may include, for instance, the need to pursue our legitimate interests (for example, providing educational offerings and conducting admissions analysis); to process transaction requests made by students, and meet our obligations (for example, to process application for admission); compliance with a legal obligation as necessary (for example, financial aid reporting); or on the basis of a student's consent, where applicable.

A.4 How Personal Data is Used if Admitted

If admitted to one of Cooper Union's three schools a student's Personal Data will be shared as necessary for registration and enrollment. Personal Data may also be shared as necessary to administer and deliver a student's education and related activities with other persons or entities, including Cooper Union's departments, faculty and staff, financial aid sources, and governmental authorities. For example, a student's name and other contact information may be shared with a professor in whose course they enroll, to administer financial aid, or for other reasons consistent with Cooper Union's efforts to provide educational services.

B.1 Alumni and Donors

Commented [AT9]: Terri, Jennifer Durst, Kim Newman to review

Cooper Union collects and uses various kinds of Personal Data about alumni, donors, and prospective donors from several sources, including data provided to us, for example, when updating the alumni or donor profile, connecting through social media, completing a contribution form, or registering to attend Cooper Union events. For those who studied at Cooper Union and their parents, some personal data is transferred from the student and application records into the alumni database. The Alumni Affairs and / or Development Office may also collect Personal Data from publicly available sources or third-party sources that support its operations. The Personal Data collected is used for the primary purpose of providing opportunities to engage with alumni, donors, prospective donors and students through interactions, events and gifts or donations. We may disclose data to other Cooper Union entities and individuals such as alumni clubs, shared interest groups,

or volunteers in connection with the purposes described below, but only after a confidentiality agreement is signed.

B.2 Personal Data Collected in conjunction with Alumni and Donor Records include:

Cooper Union and / or its third-party vendors may collect:

- **Alumni data:** is collected on a voluntary basis and made available through a password protected portal. Profile information includes directory information, preferred class year and school. Alumni have the ability to opt out. This voluntary data is stored separately from data used for administrative purposes.
- **Contact Information**: for example, name, home address, email address, phone number and social media profiles and usernames; and links to LinkedIn profiles;
- **Demographic Information**: for example, gender, age, and other information voluntarily provided;
- **Personal Information and History**: for example, personal interests, charitable activities, other personal information voluntarily provided as well as other information we may learn about your background;
- **Education History**: for example, prior and subsequent schools, awards, honors, and student activities;
- **Employment Information**: for example, title, employer, location, and work experience;
- **Cooper Union Affiliations**: for example, social network, group memberships;
- **Financial Information**: for example, contribution history, publicly available data on wealth and assets, and contributions to other organizations;
- **Transaction Information**: Cooper Union does not store payment information. A third-party service that handles credit card and wire transfer transactions. A record of each transaction is stored with the date, amount and a fragment of the payment information (i.e. last 4 digits of the credit card number).
- **Contribution History**: Contribution history to Cooper Union;
- **Your Image**: for example, when a photograph or other image is used in online networking or announcements, or when participating in events that are recorded by photography or video;
- **Family and Relationship Information**: for example, family member names, ages, occupations; additionally non-familial personal and professional relationship between records that are pertinent to operations.
- **Log Files, Cookies, Location Information, and Mobile Device Sensor Information**: When using our websites or mobile applications, we also may collect additional information about alumni and donors, and their devices as described in the "Websites and Mobile Applications" section.

Commented [AT10]: Needed from IT_Marget

B.3 The Purpose of Collecting this Information as it pertains to Alumni/Donors:

Personal Data is processed as part of Cooper Union's alumni and donor outreach and services, to:

- Provide alumni, donors, and their families the opportunities to engage with Cooper Union alumni and students;
- Facilitate alumni and donor communications, events, fundraising (including identifying prospects) and operations;
- Request and process contributions;
- Communicate about opportunities for giving, and to understand alumni/donor interests and explore support of The Cooper Union through volunteerism and philanthropy;

- Improve alumni and donor services, analyze engagement and contribution trends, and personalize the engagement experience;
- Satisfy legal, regulatory, and contractual obligations; or
- Engage in other activities as described under "Additional Uses of Personal Data."

Personal Data is processed for the purposes described above consistent with the legal bases recognized by the Relevant Law in each Relevant Country, which may include, for instance: to pursue legitimate interests (for example, requesting gifts or donations); to process transactions requested by alumni and donors; and meet our contractual obligations (for example, registration for events or processing of donations); as necessary for compliance with a legal obligation (for example, to provide required tax information); or on the basis of alumni / donor consent, where applicable.

C.1 Online Engagement

Personal Data is collected when one applies or registers for online education offerings, offered using the Teams© platform. Personal Data is also collected when one participates in online courses, programs, and activities. In some cases, the collection of Personal Data through online education activities takes place as part of a "hybrid" or "continuing education" program in which you also may participate in person, or as part of remote learning occurring in a course or program that is ordinarily conducted in person.

C.2 Personal Data Collected in conjunction Online Engagement include:

The Personal Data collected is used for the primary purposes of providing online education, and, if applicable, evaluating a student's qualification for related certificates or course credit. Cooper Union and our third-party vendors may collect:

- **Contact Information**: for example, name, home address, email address and phone number;
- **Payment Information**: depending on the means of payment, a payment card number or bank and bank account number, and government identification number where legally required;
- **Demographic Information**: for example, gender, age, and date of birth;
- **Personal Information and History**: for example, personal interests, other information volunteered in profiles or otherwise in the online platform, and other information we may learn about your background;
- **Education Information**: for example, schools, transcripts, awards, and honors;
- **Employment Information**: for example, title and employer, history, and work experience;
- **Learner Interaction and Participation Data**: for example, exchanges with other learners, discussion and forum contributions, course posts, and participation in class sessions or other online events that are transmitted or recorded in audio and/or visual form;
- **Course Engagement and Assessment Data**: for example, assignment responses, test scores, and course interactions (such as engagement with peers and faculty in the online environment);
- **Log Files**: for example, in engaging online, we collect IP address, browser type, internet service provider, pages visited (including referring/exit pages), operating system, date/time stamp and/or clickstream data;

Commented [AT11]: Robert - need to write statement about destruction of online teams/class records

- **Cookies and Similar Technologies**: information collected automatically through cookies and similar technologies when interacting online. For more information regarding our use of cookies and similar technologies, see the "Cookies and Similar Technologies" in the Website engagement section;
- **Your Image**: for example, where you voluntarily provide a photograph or other image for use in an online course or program (for example, in a profile), or where you appear in a video transmission or recording.

Commented [AT12]: · **Mobile Device Sensor Information**: mobile applications may use various sensors and components of mobiles device (for example, your camera or microphone) to collect information for the purposes of providing you with additional functions and features; and

C.3 The Purpose of Collecting this Information as it pertains to Online Engagement:

Personal Data for online education is collected to:

- Provide and administer the course, program or activity including the ability to evaluate success in and engagement with the online education offering;
- Respond to requests and communicate with students regarding current or future courses, programs, or activities;
- Provide services related to courses, programs, or activities;
- Conduct research (for example, in the areas of education) and analytics related to online educational offerings;
- Satisfy legal, regulatory, and contractual obligations; or
- Engage in other activities described under "Additional Uses of Personal Data" below.

Personal Data is processed for the purposes described above consistent with the legal bases recognized by the Relevant Law in each Relevant Country, which may include, for instance: to pursue Cooper Union's legitimate interests (for example, providing educational offerings and evaluating performance); to process transactions requested by students and to meet contractual obligations (for example, to register students for an online educational course or experience); as necessary for compliance with a legal obligation; or on the basis of consent, where applicable.

D.1 In Person Educational Programs conducted with Relevant Countries

Cooper Union conducts certain educational programs with Relevant Countries, including exchange and undergraduate research programs. Cooper Union collects Personal Data to administer these offerings. Personal Data collected by Cooper Union or on our behalf, are used for the primary purposes of providing educational offerings and, if applicable, evaluating qualification for certificates and credit.

D.2 *In Person* Data Collected in conjunction with Educational Programs conducted in Relevant Countries:

Cooper Union and third-party vendors may collect:

- **Contact Information:** for example, name, home address, email address and phone number;
- **Payment Information**: depending on means of payment, payment card number or bank and bank account number, and government identification number where legally required;
- **Demographic Information**: for example, gender, age, and date of birth;

- **Personal Information and History**: for example, personal interests, profession, and other information about your background;
- **Education Information**: for example, schools attended, transcripts, school activities and disciplinary records, awards, and honors;
- **Employment Information**: for example, title and employer, employment history and work experience;
- **Course Assessment Data**: for example, assignment responses, test scores and course evaluations;
- **Learner Participation Data**: for example, your participation in class sessions or other online events that are transmitted or recorded in audio and/or visual form;
- **Residential Information**: for example, local host information for exchange and study abroad, and personal preferences that have been voluntarily provide;
- **Log Files, Cookies, Location Information**: When using Cooper Union websites or mobile applications, we also may collect additional information as described in the "Websites and Mobile Applications" section.

D.3 The Purpose of Collecting this Information as it pertains to Educational Programs conducted in Relevant Countries:

An application for non-matriculated programs is secured. Cooper Union processes Personal Data relating to in-person or hybrid educational programs in Relevant Countries, to:

Commented [AT13]: Secure samples from SoE, SoArt, SoArch and Cont Ed Typographics and Type@Cooper.edu

- Provide and administer the course or program in which the student or faculty is participating, including sharing information about you with other participants, providing academic guidance and evaluating success in the course or eligibility for certification;
- Provide services related to the course or program;
- Respond to requests and communicate regarding current or future courses or programs;
- Conduct analytics to improve educational offerings at The Cooper Union;
- Satisfy legal, regulatory, and contractual obligations; or
- Engage in other activities described under "Additional Uses of Personal Data."

Cooper Union processes Personal Data for the purposes described above consistent with the legal bases recognized by the Relevant Law in each Relevant Country, which may include, for instance: to pursue legitimate educational interests (for example, conducting analytics to improve program offerings); to process transactions requested by students and meet contractual obligations (for example, providing educational programs); as necessary for compliance with a legal obligation; or on the basis of consent, where applicable.

- **E.1 Research**

Cooper Union researchers, research collaborators, partners and service providers may collect, use, and share Personal Data as part of a research study in which the student/faculty participates as a research subject, or in which existing data are used. It is generally the case that before any Personal Data are collected for research purposes, students are provided a consent and/or authorization form for the specific research project that explains the types of data collected and the purposes for which such data will be processed and shared. In these cases, the description of the collection and use of Personal Data provided in the consent and/or

authorization form will replace the information provided herein. The Personal Data collected by researchers, research collaborators, partners, and service providers, or on their behalf, are used for the primary purposes of furthering the research project and more generally for supporting research and understanding in fields of academic study.

Examples of Personal Data that may be collected for research purposes are listed. Questions about the processing of personal data in connection with a research study should be directed to those who are conducting the research, or the contact persons named in any consent form signed upon joining the study.

E.2 Research Data Collected:

Examples of Personal Data that Cooper Union and / or third-party collaborators or service providers may collect for research purposes include the following. Please note that in most cases these data, if identifiable, would initially be provided voluntarily by you:

- **Contact Information**: for example, name, home address, email address and phone number;
- **Payment Information**: bank and bank account number, and government identification number where legally required, for processing compensation if being paid in connection with the research;
- **Demographic Information**: for example, race, ethnicity, gender, age, education, profession, occupation, income level and marital status, photo, or another image;
- **Personal Information and History**: for example, personal interests, profession, and other information about your background;
- **Family Information**: for example, family members, ages, occupations, and health;
- **Employment History**: for example, employers, titles, wages, work experience, trade union membership and disciplinary record;
- **Education History**: for example, schools, transcripts, awards, honors, and disciplinary records;
- **Research specific data**: such as biometrics, sensor, or genetic information;
- **Course Engagement and Assessment Data**: for example, assignment responses, test scores and course interactions;
- **Log Files**: for example, IP address, browser type, internet service provider, pages visited (including referring/exit pages), operating system, date/time stamp and/or clickstream data;

Commented [AT14]: Marget please review

- **Cookies and Similar Technologies**: Information collected automatically through cookies and similar technologies. For more information regarding our use of cookies and similar technologies, see the "Cookies and Similar Technologies" section in the "Website and Mobile Applications" section; and

A Memorandum of Agreement, MOA, is secured for research initiatives. Additionally, Cooper Union may collect the contact, payment, employment and education information of researchers, research partners or collaborators and service providers to administer the study and manage the relationship and compensation.

Commented [AT15]: Secure samples of research contracts

Commented [AT16R15]: Request review from SoE

E.3 The Purpose of Collecting this Information as it pertains to Research Projects:

Personal Data is processed for research in accordance with the purposes of the research projects and funder requirements, and to also:

- Further scholarship, research and understanding in fields of academic study pertinent to Cooper Union's academic programs;
- Enroll research subjects in particular research study;
- Administer the study in keeping with funder and agency requirements;
- Report to project funders and other project participants;
- Satisfy legal compliance requirements; or
- Provide required reports to tax authorities on payments to research subjects, researchers, and service providers.

Cooper Union processes Personal Data for the purposes described above consistent with the legal bases recognized by the Relevant Law in each Relevant Country, which may include, for instance: to pursue our legitimate interests (for example, growing scholarship and conducting research); to process transactions and meet our contractual obligations (e.g., paying faculty, employees, research collaborators and research subjects); as necessary for compliance with a legal obligation (for example, to comply with Institutional Review Board, IRB, standards, report adverse events to regulatory authorities like the National Science Foundation and National Institute of Health, that oversee the safety of medical products and research); as necessary for the performance of tasks we carry out in the public interest (for example, to further research and understanding in fields of academic study); where processing is necessary for scientific or historical research purposes and performed consistent with required data protection safeguards; or on the basis of your consent, where applicable.

F.1 Employees, Job Applicants and Service Providers

Personal Data is collected when one applies to work for Cooper Union in a Relevant Country. Further Personal Data collection occurs at hiring and throughout one's relationship with The Cooper Union. We may also collect Personal Data about personnel of vendors providing services to us in a Relevant Country.

Commented [AT17]: Natalie to review statements and identify other information

The Personal Data collected by Cooper Union, or on our behalf, are used for the primary purposes of providing employment, engaging with service providers, legal compliance, and enabling employees and service providers to utilize our services, facilities, and engage with Cooper Technologies as specified by the information technology office.

F.2 Personal Data Collected:

Cooper Union may collect the following information:

- **Contact Information:** for example, name, preferred name, home address, email address and phone number;
- **Payment Information:** bank and bank account number for processing compensation;
- **Tax Information**: for example, government identification number, wages and filing status;

- **Personal Information and History**: for example, marital status and other information about your background, and when relevant for the position or required by law, credit history, driving record, self-reported and publicly available criminal records, citizenship, and work authorization status;
- **Demographic Information**: for example, gender, age, and date of birth; we also request information about ethnicity and race, which is voluntary for the purposes of surveys/demographic reporting
- **Employment and Work History**: for example, prior employers, titles, wages, work experience and disciplinary record;
- **Education Information**: for example, schools, transcripts, awards, honors, and disciplinary records;
- **Family Information**: for inclusion in benefits plans;
- **Medicare enrollment information** – for retirees, in order to transition their coverage, or reimburse them for premiums (if eligible)
- **Health Information**: for example, medical information voluntarily provided would support a request for accommodations;
- **Image**: for example, a photograph or other image will be used for Cooper identification cards or in announcements;
- **Log Files, Cookies, Location Information, and Mobile Device Sensor Information**: When you use our websites or mobile applications, we also may collect additional information about you and your device as described in the "Websites and Mobile Applications" section above.

F.3 The Purpose of Collecting this Information as it pertains to Employment, Job Application or in Providing a Service:

Personal Data for employment or other work relationship and job application purposes is used to:

- Evaluate the application for employment or other work relationship and communicate hiring decisions;
- Engage with service providers;
- Administer and facilitate workforce-related processes and operations, including compensation processing and the provision of employee benefits;
- Provide support services, including accommodation;
- Satisfy legal, regulatory, and contractual obligations;
- To engage in other activities described under "Additional Uses of Personal Data."

Cooper Union uses Personal Data for the purposes described above consistent with the legal bases recognized by the Relevant Law in each Relevant Country, which may include, for instance: to pursue legitimate interests regarding hire and employment (for example, managing internal administrative tasks); to process transactions requested and meet contractual obligations (for example, managing employment or other work relationships); as necessary for compliance with a legal obligation (for example, to provide required information to tax authorities); or on the basis of consent, where applicable.

G. Additional Uses of Personal Data:

The use of personal data for other purposes may result from consent by the faculty, staff, or student; or may be required in the effort to fulfill contraction obligations, federal regulations, legal compliance or to pursue legitimate interest:

- Conducting our in-scope operations and administering and developing educational offerings;
- Administering fellowships, grants, and other programs in support of individual study and research projects;
- Responding to requests for research assistance;
- Processing and responding to requests or inquiries of any other kind;
- Providing newsletters, articles, service alerts or announcements, event invitations, volunteer opportunities, and other information that we believe may be of interest to you;
- Requesting gifts and donations;
- Processing and fulfilling requested transactions for merchandise or other Cooper Union products;
- Alerting constituents about a safety or security announcement;
- Conducting research, surveys, and similar inquiries to support the ability to understand trends and needs of our applicants, students, and others;
- Meeting the requirements of our accreditors;
- Disclosing directory information as described in FERPA<LIN K>;
- Performing marketing, promotions, and advertising, either directly or through third parties (such as Survey Monkey). These activities may include interest-based advertising, targeted advertising, and online behavioral advertising to increase the likelihood that the content will be of interest;
- Ensuring the rights, safety and security of our students, faculty, fellows, employees, and others;
- Preventing, investigating, taking action regarding or providing notice of fraud, unlawful or criminal activity, other misconduct, security or technical issues, or unauthorized access to or use of Personal Data, the website, or data systems;
- Responding to subpoenas, court orders, or other legal processes; fulfilling and enforcing our agreements and legal rights; protecting the health, safety, rights, or property of you, us, or others; and meeting legal obligations.

H.1 Personal Data and Third-Party Providers: Sharing Data

Cooper Union uses partners and service providers, such as admissions application facilitators (for example, the Common Application and the College Board), payment processors (for example, TouchNet), analytics providers (for example, Google and Qualtrics), and platform providers (for example Microsoft) to provide services for us. Some of these partners have access to Personal Data that we may not otherwise have (for example, when you sign up directly with that provider) and may share some or all this data with Cooper Union. Institutional data and data sharing may be protected by several laws, regulations, and policies and procedures including but not limited to the Family Educational Rights and Privacy Act (FERPA), EU General Data Protection Regulation (GDPR), Gramm Leach Bliley Act (GLBA) depending on the data source, data subjects, and purpose of the data processing.

Cooper Union's Finance Officer is the signatory on data use agreements (DUAs) involving the processing (including creation, use, control, or sharing) of Cooper Union institutional data by external entities and all

Memorandums of Agreement (MOAs). A Data Use Agreement ("DUA") is a binding contract governing access to and treatment of nonpublic data provided by one party (a "Provider") to another party (a "Recipient"). DUAs are often required by external parties before they permit data to be received by Cooper Union and may also be necessary for Cooper Union data to be disclosed to another organization.

An authorized signature is required on agreements involving the processing of data to ensure that the appropriate laws, regulations, policies, procedures, and requirements necessary to protect Cooper Union's institutional data have been addressed within the data sharing agreement, and the privacy of our constituents protected.

Commented [AT18]: Secure Data Sharing agreement - this is needed for federal proposals - likely one as tNS

- **Sharing Information:** Cooper Union shares information with internal stakeholders who have a *need to know* to support institutional operations, "in scope processing." There are also external service providers, institutions and research partners, and other collaborators with which personal data may be shared. Cooper Union reviews, approves, and signs data agreements when sharing institutional data with external entities (for instance Exchange Program Agreements and Research Exchanges).

Commented [AT19]: Check with Keith

Commented [AT20R19]: More information needed?

- **Single Sign On**: Some of Cooper Union's online offerings or research activities may allow one to register and login through a third-party platform. When "logging in" to Cooper Union's offering or activity through a third-party platform, the user allows us to access and collect any Personal Data from their third-party platform account as permitted under the settings and privacy statement of that platform.

H.2 Other Providers and Collaborators

- **Service Providers**: Personal data with third-party service providers that complete transactions or perform services on our behalf or for your benefit, including, but not limited to, the following:

Commented [AT21]: Gets systems and maintain list

  - Educational or research operations and collaborations such as with exchange programs or survey providers;
  - Course tools that support educational offerings such as Microsoft Teams;
  - Enrollment verification and transcript services;
  - Facilitating other transactions
  - Payment and contribution processing;
  - Processing admissions and financial aid applications;
  - Student, alumni, and donor outreach and engagement;
  - Social networking, email, and communications services;
  - Human Resources administration and operations;
  - System maintenance, security, and other technology services;
  - Marketing and data analytics;
  - Facilitating federal and state compliances; and
  - Legal compliance.

- **Other Institutions & Collaborators**: Cooper Union may share personal data with other institutions for the purposes of delivering programs and services including, but not limited to, the following:

- Registration, enrollment verification and coordination for courses and events, including cross-registration for courses and events with other universities;
- Library exchange programs;
- Course administration, evaluation, and assessment;
- Study at other universities, including study abroad at foreign universities;
- Hybrid education offerings through software platforms;
- Research arrangements with other universities or collaborators; and
- Events and activities of Cooper Union clubs and special interest groups.

Commented [AT22]: Verify with Lisa Norberg

Cooper Union may disclose Personal Data to legal or government regulatory authorities as required by law. We may also disclose Personal Data to third parties in connection with claims, disputes, or litigation, when otherwise required by law, or if it is determined that disclosure is necessary to protect the health, safety, rights, or property of users, us, or others, or to enforce Cooper Union's legal rights or the contractual commitments that you have made.

- **Third Parties in Connection with Claims:** Cooper may also disclose personal data to third parties in connection with claims, disputes, or litigation, or when we believe, in good faith, that such release is necessary to:
  - Comply with applicable law;
  - Enforce or apply the terms of any of user agreements;
  - Protect the rights, property, or safety of Cooper Union or any School, the Faculty of the Humanities, department, program, or offices affiliated with Cooper Union, our users, or others;
  - Enforce our legal rights or contractual commitments that you have made.

- **Website, Cookies and Similar Technologies:** When engaging with the Cooper Union websites or otherwise providing information to us, the user consents to the collection, use, and disclosure of their information in accordance with this Policy. Whenever visiting or using our websites or online services, Cooper Union may deploy cookies and related technologies ("Cookies") to collect certain personal information about you. We use the information to enhance and personalize the experience, support our ability to provide services, analyze website and service usage, and help improve the websites and our related services. Students are referred to the Cooper Union Cookie Statement for an overview of Cookies on our websites.<link to Cooper Union Cookie Statement> , addressing why we use cookies and types of cookies, as well as guidance on how to change cookie settings.

  Third parties may also use Cookies embedded in our sites to collect information about your online activities over time and across different websites you visit. This information may be used by third parties to provide advertising tailored to your interests on other websites, apps, and services you visit.

Commented [AT23]: Marget can have at this!!!

You can review your Internet browser settings, typically under the sections "Help" or "Internet Options," to exercise choices you have for certain Cookies, or you can opt out of the collection and use of some Cookies through tools like the Network Advertising Initiative opt-out page. If you disable or delete certain Cookies in your settings, you may not be able to use features of our websites. More information about cookies is available, visit https://www.internetcookies.org/.

- **Analytic Services:** Cooper Union may use third party analytics such as Google Analytics or similar analytics services. For information on how Google processes and collects information using Google Analytics, please see www.google.com/policies/privacy/partners/, and for how to opt out, please see https://tools.google.com/dlpage/gaoptout.

  The opt-outs described above may not work for all browsers or devices. If you have any questions regarding the use of cookies and other similar technologies, please contact us as set forth in the "Contact Us" section below.

- **Social Media Platforms:** Cooper Union may also use services provided by third parties (such as social media platforms) to serve targeted ads or sponsored content on third-party platforms. An additional note about **Social Media**: If you share Cooper Union content through social media, such as liking us on Facebook, interacting with us on LinkedIn or Instagram, or tweeting about us on Twitter, those social networks will record that you have done so and may set a cookie for this purpose. If you wish to opt-out of any of these social interactions, please refer to the specific social media platform for instructions on how to do so.

- **Mobile Apps????**

Commented [AT24]: Robert - do we need a comment here

PART B

This section addresses considerations in providing data subjects the ability to access, correct, amend, or delete personal information where it is inaccurate or processed in a way that violates the principles. It also addresses security measures in place to mitigate the risks associated with the management, processing, and nature of Personal Data. Personal Data will be retained for as long as is necessary for the purposes set out in these Disclosures, in accordance with Relevant Law and the legal bases for acquiring the data. For example, we may retain Personal Data as follows:

- For as long as may be required under applicable law;
- As needed to resolve disputes or protect Cooper Union's legal rights;
- Where processing is based on your consent, for the period necessary to carry out the processing activities to which you consented;
- Where processing is based on contract, for the duration of the contract plus some additional limited period that is necessary to comply with law or that represents the statute of limitations for legal claims that could arise from the contractual relationship;

- Where processing is based on the public interest, for the period that continues to serve that underlying interest.
- Where processing is based on our legitimate interests, for a reasonable period based on the particular interest, considering the fundamental interests and the rights and freedoms of the data subjects.
- In some cases, where Personal Data was processed and retained based on consent, contract, the public interest, or other bases described in these Disclosures, we may continue thereafter to retain the data based on a legitimate interest.
- Consistent with the foregoing guidance, some data may be retained indefinitely.

Access to Personal Data and Ability to Request Change and Security Measures in place to mitigate risks associated with the maintenance and administration of data.

Because data, data controllers and data processors are role specific as established in the Disclosures made in Part A, and because of data protocols and security measures established by the Information Technology office, Cooper Union as the ability to respond to requests regarding Personal Data.

To the extent required by Relevant Law, upon one's reasonable and good faith request, Cooper Union can respond to inquiries as to whether we hold Personal Data as part of the school's operational, *In-scope* Processing. If it is that *In-scope Processing* as to one's Personal Data is solely based the consent provided by students, faculty, or staff, in certain cases these constituents may also have the right under a Relevant Law to withdraw their consent to our processing.

- If consent for the use or sharing of one's Personal Data for the purposes set out in these Disclosures is withdrawn, or if the use of Personal Data is otherwise limited; or a request for its deletion is advanced; Cooper Union may no longer be able to provide some or all the related services explained herein.
- Please note that, in certain cases, Cooper Union may continue to process one's Personal Data after they have withdrawn their consent or requested that their Personal Data be deleted, if the school has a legal or regulatory basis to do so. For example, we may need to retain certain data to comply with an independent legal obligation, for achieving the lawful purposes for which we obtained the data, or for such reasons as keeping our services and operations safe and secure or safeguarding our rights or the rights or safety of others.

Thus upon making a reasonable, good faith request, Cooper Union will provide constituents with information about whether any of their personal data is held as part of Cooper Union's GDPR processing activities, to the extent required and in accordance with applicable law.

- In certain cases, you may also have a right, with respect to your personal data collected and used in GDPR processing activities, to:
- Access your Personal Data held by Cooper Union;
- Correct inaccurate or incorrect information about you;
- Request erasure of information when it is allowable and no longer necessary for us to retain it;
- Restrict processing of your personal information in specific situations;

- Object to the processing your information, including sending you communications that may be considered direct-marketing materials;
- Object to automated decision-making and profiling, where applicable; and
- Complain to a supervisory authority in your EEA authority.

Subject to certain legal limits, constituents also have the right to withdraw their consent to our processing of their personal data as part of our GDPR processing activities, where our processing is solely based on consent. However, in certain cases, we may continue to process personal data even if consent has been withdrawn, if we have a legal basis to do so. For example, we may retain certain data if we need to process data to comply with an independent legal obligation, if we still need the data for the lawful purposes for which we obtained the data, or if it is necessary to do so to pursue our legitimate interest in keeping our services and operations safe and secure or to safeguard our rights or the rights or safety of others.

- **International Data Transfer**

Personal Data processing takes place in the United States, although there may be occasions in which Cooper Union, or third parties with whom we share data, may process data in other countries. The data protection laws in the United States and other countries may provide less protection than such laws in one's Relevant Country. In the event we transfer one's Personal Data outside their Relevant Country as part of our In-scope Processing, we rely, where required on appropriate or suitable safeguards or specific legal provisions permitting such transfers under the Relevant Law.

When transferring Personal Data from a country in the European Economic Area ("EEA," European Union member states, Norway, Liechtenstein, and Iceland), we acknowledge the rights granted to you under the GDPR. If you are located in the United Kingdom (U.K.), which has left the European Union, but has adopted legislation substantially similar to the GDPR, we acknowledge the rights granted to you under the Data Protection Act of 2018) or from the United Kingdom (UK) to a country outside the EEA and the UK, we may base such transfers on contracts containing legally authorized data protection clauses referred to as **Standard Contractual Clauses**.

GDPR rights requests are centrally managed through the office of Information Technology. This ensures consistency, transparency, and accountability in Cooper Union's response to requests regarding Personal Data and to ensure the protections that protect the privacy and security of data.

3. The Gramm Leach Bliley Act

Background

The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999 (15 USC §§ 6801 et seq.), was designed to regulate the disclosure and protection of non-public personal information (NPI) collected by a financial institution from an individual in order to obtain a financial product or service from the institution for personal, family, or household purposes. All information submitted for financial aid is

protected under Cooper Union's privacy policies, including FERPA, GDPR and the Gramm-Leach Bliley Act of 1999. Under these provisions, Cooper Union ensures the privacy and safeguarding of all financial aid information.

The Federal Trade Commission (FTC) is charged with administration and enforcement of the GLBA for financial institutions not regulated by other federal banking or finance-related authorities, including institutions of higher education (IHEs). The FTC has determined that most IHEs are "financial institutions" for purposes of the GLBA because "[m]any, if not all, such institutions appear to be significantly engaged in lending funds to consumers." 64 Fed. Reg. 33648 (May 24, 2000). In addition, the Department of Education requires IHE compliance with the Safeguards Rule by contract, under the Federal Student Aid (FSA) Program Participation Agreement and Student Aid Internet Gateway (SAIG) Agreement.

GLBA Act

The three major components of the GLBA include:

- The "Pretexting Provision" (15 USC § 6821), which prohibits the solicitation or disclosure of NPI by false pretenses or deception;
- The "Financial Privacy Rule" (16 CFR Part 313), which governs the collection and disclosure of NPI and requires written notice of the institution's privacy practices and policies; and
- The "Safeguards Rule" (16 CFR Part 314), which requires a documented assessment of internal and external risks to NPI and implementation and maintenance of a comprehensive information security program that addresses these risks. The Safeguards Rule was effective May 23, 2003.

The Pretexting Provision of the GLBA is addressed in the Federal Trade Commission's "Red Flags Rule" (16 CFR § 681.1), that was established after the Financial Privacy and Safeguards Rules in connection with amendments to the Fair Credit Reporting Act (FCRA) (15 U.S.C. § 1681). CU must also comply with this distinct, but related, rule that requires implementation of an identity theft prevention program related to "covered accounts." The original Red Flags Rule was effective November 1, 2008.

For more information about Cooper Union's "Red Flag" rule, please review "Cooper Union's Red Flags Identity Theft Protection Program" policy.

The Financial Privacy Rule provides that institutions of higher education that comply with the Family Educational Rights and Privacy Act (FERPA) to protect the privacy of education records – including student financial aid records – are deemed to comply with the rule. For more information, please review "Cooper Union's Family and Educational Rights Act," FERPA.

GLBA Implementation

The Gramm-Leach-Bliley Act, (GLBA) effective May 23, 2003, addresses the safeguarding and confidentiality of customer information held in the possession of financial institutions such as banks and investment companies. GLBA contains no exemption for colleges or universities. Cooper Union must comply with the

Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act, or GLBA) and specifically with the GLBA Safeguarding Rule issued by the Federal Trade Commission. This applies to safeguarding customer information for loans to students, and / or parents/guardians. It may apply to other financial transactions involving customer information. The objectives of the GLBA Safeguards Rule are to:

- Ensure the security and confidentiality of customer information, including non-public personal information, NPI.
- Protect against any anticipated threats or hazards to the security of such information.
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to customers.

To comply, Cooper Union must develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards appropriate to the organization's size and complexity, nature, and scope of activities, and sensitivity of NPI at issue.

The following requirements have been put in place:

- An IT employee dedicated to coordinating the information security program.
- A risk assessment to identify, within reason, foreseeable internal and external risks to the security, confidentiality, and integrity of customer information (including NPI) that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and the assessment of the sufficiency of any safeguards in place to control these risks. At minimum, the risk assessment must include consideration of risk in each relevant operational area, including:
    - Employee training and management.
    - Information systems, including network and software design, information processing, storage, transmission, and disposal.
    - Detecting, preventing, and responding to attacks, intrusions, or other system failures.

- Implementing information safeguards to control identified risks and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures.
- Overseeing service providers by taking reasonable steps to select and retain providers capable of maintaining appropriate safeguards for NPI and requiring them by contract to implement and maintain such safeguards.
- Evaluating and adjusting the information security program considering the results of the required testing/monitoring, any material changes to operations or business arrangements, or any other circumstances that may have a material impact on the program.

Details of steps taken to protect privacy are provided in the Data Privacy policy and specifically, Data Management and Data Security.

- **Non-Public Information**

To comply with the GLBA, the Cooper Union is required to implement an information security program that incorporates administrative, technical, and physical safeguards appropriate our size and organization, nature and scope of activities, and sensitivity of the non-public information under consideration. The various administrative, technical, and physical safeguards implemented in connection with Cooper Union's comprehensive Data Governance and Information Technology (IT) Security programs are consistent with, and support, GLBA Safeguards Rule compliance.

Following are examples of NPI that may be obtained in connection with the delivery of a financial product or service:

- Account balances
- ACH numbers
- Bank account numbers
- Credit card numbers
- Credit ratings
- Date and/or location of birth
- Driver's license information
- Family Income information
- Income history
- Payment history
- Social Security numbers
- Tax return information
- Name, address, phone number on an application for financial aid

Cooper Union's administrative units that collect/maintain protected NPI that must be protected under the regulations established by Gramm Leach Bliley are involved in the servicing of student loans, payment plans, and coordinating with collection agency services. These Units are collecting or processing NPI information to provide a financial process or service and must comply with GLBA and safeguards established in the privacy policies and practices established by IT, most importantly when acquiring protected data. This holds true even when the unit is not primarily responsible for operating on the information.

Examples of a financial product or service covered by the GLBA regulations: The making or servicing of student loans or financial aid.

- The provision or guarantee of loans under the Faculty Housing Assistance Program.
- Any extension of credit for personal or family purposes (such as an extension of credit for tuition, fees, housing, or medical services) as in payment plans

Non-Public Information must be safeguarded in paper and electronic forms by all and any administrative units (entities) with access to NPI data, including across shared data record systems regardless of whether the entity is extending credit or awarding financial aid. Cooper Union's financial offices:

- Maintain and review internal policies and procedures to ensure that they have put appropriate administrative, technical, and physical safeguards in place.
- Train staff on how to safeguard sensitive (NPI) data to ensure they are aware of the steps to respond and report to potential threats to the information system, educational records and NPI.
- Review contracts with service providers that collect or have access to NPI to ensure that protocols are in place to safeguard information.

The Information Technology office conducts risk assessment to identify and oversee service providers. In conjunction with the procurement office, IT is deliberate when selecting and retaining providers to support finance operations to assure the privacy and security safeguards needed to protect NPI. Service provider contracts include appropriate assurances regarding the safeguarding of sensitive personal information, including NPI, consistent with the requirements of the Rule and other applicable law.

Although it may be that many administrative units at Cooper Union are not involved in the processing of financial information it is nonetheless important that all administrative and academic units be made aware of the regulation and the privacy practices put in place by Cooper Union.

4. The New York SHIELD ACT

The SHIELD Act has substantially expanded the definition of private information to include -- in addition to social security numbers, driver's license numbers, credit or debit card numbers, or financial account numbers -- to include biometric information, email addresses, and corresponding passwords or security questions.

Commented [AT25]: Robert - these are likely included in the data protection strategy, but we should verify~

The SHIELD Act requires any person or business that maintains private information to adopt administrative, technical, and physical safeguards to protect private information.

A. Reasonable adminstrative safeguards undertaken by The Cooper Union are established in the data management and governance practices established herein. They include:

- Designating one or more employees to coordinate the securty program
- Identifying reaonabilty forseeable inernal and external risks which are provided in Cooper Union's security strategy. The office of Information Technology conducts an annual assessment of systems, software, processes, and potential breaches; data transmission protocols.
- Assessing on an annual basis of the sufficiency of safeguards in place to control identified risks is conducted.
- Conducting training and managing key employees in the security programs and protocols.
- Establishing appropriate safeguards in service contracts with external providers.

B. The Cooper Union has put in place reasonable technical safeguards to protect personal data. They include, the:

- Assessment of risks associated with information storage and disposal.

- Detecting, preventing and responding to security risks and threats.
- Protecting against unauthorized access to our use of private information during or after the collection, transportaiton and destruction or disposal of private records.
- Disposing of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed

Through ongoing assessment and management input, Cooper Union's IT departement will update its security plan as needed. Should there be a breach in the security systems that affects private information, Cooper Union's data governance and information security plan establishes that it will notify affected entities (consumers) in the most expedient way possible consistent with the legitimate needs of law enforcment agencies. To comply with the NY Shield act law which requires notice to the Office of the New York State Attorney General (OAG), the New York Department of State, and the New York State Police of the timing, content, and distribution of the notices and approximate number of affected persons, The Cooper Union is required to submit breach form through the Office of the Attorney General's data-breach-reporting portal.

V. Associated Policies and Materials

- The Cooper Union Cookie Statement
- The Family and Educational Rights and Privacy Act, FERPA
- The General Data Protection Regulations, GDPR
- GDPR Notice
- The Gramm Leach Bliley Act, GLBA
- The Cooper Union Red Flag Identity Theft policy
- New York Sheild Act