Privacy Framework

May 2024

King's University College
Information Technology Services
Dominique Perreault

KING'S
Western University

King’s Privacy Framework

Executive Summary

This Privacy Framework is a comprehensive document that outlines the principles, policies, and procedures to govern the protection of personal information within the organization, King’s University College (King’s).

Privacy has become a critical concern in today's digital age, and as an organization, King’s recognizes the importance of safeguarding the personal information of its stakeholders, including students, faculty, staff, and external partners. This Privacy Framework will serve as a roadmap to ensure that privacy considerations are integrated into all aspects of King’s operations and is built on the following foundational elements:

Privacy Principles: King’s has defined a set of privacy principles that guide its approach to personal information handling. These principles emphasize accountability, consent, limiting collection and use, data accuracy, safeguards, openness, individual access, and compliance.

Personal Information Management: The Privacy Framework outlines processes for the collection, use, disclosure, retention, and disposal of personal information. It establishes clear guidelines on how personal information is handled at every stage, from collection to destruction.

Data Security and Privacy Safeguards: King’s has implemented robust security measures and safeguards to protect personal information from unauthorized access, use, disclosure, alteration, or destruction. The Privacy Framework details these measures and highlights the importance of ongoing risk assessments and data breach response procedures.

Consent and Individual Rights: King’s respects the rights of individuals to control their personal information. The Privacy Framework provides guidance on obtaining informed consent, managing consent preferences, and facilitating individual access to personal information.

Privacy Training and Awareness: King’s prioritizes privacy education and awareness among its constituents. The Privacy Framework includes provisions for privacy training programs, ensuring that all staff and faculty members understand their responsibilities and the importance of maintaining privacy standards.

Compliance and Governance: The Privacy Framework ensures compliance with relevant privacy laws, regulations, and industry standards. It establishes a governance structure with clearly defined roles and responsibilities for privacy management, and it outlines mechanisms for ongoing monitoring, reporting, and policy updates.

This clear and concise framework provides many benefits including:

Enhanced Privacy Protection: The Privacy Framework ensures that personal information is handled with the utmost care and in compliance with applicable laws and regulations. This helps build trust with King's stakeholders and reinforces its commitment to privacy protection.

Risk Mitigation: By implementing strong privacy controls and safeguards, King's ensures the mitigation of risks associated with data breaches, unauthorized access, and non-compliance. This protects the organization from reputational damage, legal liabilities, and financial losses.

Stakeholder Confidence: The Privacy Framework demonstrates King's dedication to privacy and data protection, instilling confidence in its stakeholders. This can lead to increased student enrollment, strengthened partnerships, and improved relationships with staff and faculty.

Alignment with Best Practices: The Privacy Framework is designed to align with industry best practices and evolving privacy standards. This ensures that King's remains up to date and adaptable in addressing emerging privacy challenges.

Continuous Improvement: The Privacy Framework establishes a framework for ongoing policy review, evaluation, and improvement. It enables King's to adapt to changing privacy landscapes, emerging technologies, and stakeholder expectations.

In conclusion, the Privacy Framework is a vital tool for safeguarding personal information within the organization. By establishing clear policies, procedures, and accountability measures, King's can maintain the privacy and trust of its stakeholders while meeting legal obligations. The Privacy Framework represents King's commitment to upholding privacy standards and ensuring the responsible handling of personal information.

Contents

Introduction

1.1 Purpose

The purpose of this Privacy Framework is to provide a structured and comprehensive approach to developing, implementing, and managing policies within King's. It serves as a guiding document that outlines the principles, values, and rules that govern operational decision-making, and actions related to specific areas of concern. The key purposes of the Privacy Framework are to ensure that policies are aligned with King's mission, vision, and strategic objectives. It establishes a cohesive and consistent approach to policy development, ensuring that policies are interconnected and support the overall goals of the organization. The framework defines the roles, responsibilities, and authorities for policy development, implementation, and review. It outlines the decision-making processes, accountability mechanisms, and oversight structures that ensure effective policy governance within the organization. It provides a basis for ensuring compliance with legal and regulatory requirements, industry standards, and internal policies. By establishing policies that address specific risks and vulnerabilities, the framework supports effective risk management practices. It enables the identification, assessment, and mitigation of risks associated with various activities, promoting a proactive approach to risk management within King's environment. The framework also promotes consistency and efficiency in decision-making processes. It sets out clear procedures for policy development, review, and approval, ensuring that policies are well-structured, evidence-based, and reflect best practices. This consistency enhances organizational efficiency and reduces ambiguity in policy implementation.

The framework facilitates effective communication and transparency by providing a clear structure for policy dissemination and accessibility. It ensures that policies are communicated to relevant stakeholders, and mechanisms are in place for addressing questions, feedback, and concerns related to policies. The framework also encourages and supports a culture of continual improvement within the organization. It includes mechanisms for policy review and evaluation, allowing for regular updates and revisions to reflect changing needs, emerging trends, and lessons learned from policy implementation.

Overall, the purpose of this Privacy Framework is to establish a coherent and adaptable system for policy development and management, promoting good governance, compliance, risk management, and organizational effectiveness.

1.2 Scope

The scope refers to the boundaries and coverage of this framework in terms of the types of personal information, the individuals or entities involved, and the specific activities or processes that fall under King's purview. It outlines the areas in which the policy applies, sets expectations for privacy protection within the defined scope, and covers all activities and processes that involve personal information related to students, faculty, staff, visitors, alumni, and any other individuals associated with King's.

Personal Information Covered: The Privacy Framework applies to all types of personal information collected, processed, stored, or transmitted by the university. This includes, but is not limited to, names, addresses, contact details, identification numbers, academic records, financial information, health information, and any other data that can be used to identify or link to an individual.

Data Subjects: The Privacy Framework addresses the personal information of various individuals, including but not limited to students, prospective students, faculty members, staff members, contractors, alumni, donors, visitors, and any other individuals whose personal information is collected and processed by the university.

Collection and Processing Activities: The Privacy Framework covers all activities and processes involving personal information conducted by the university. This includes, but is not limited to, admissions, enrollment, academic records management, course registration, assessments, research activities, employment records, payroll, human resources processes, Information Technology (IT) systems, website interactions, marketing communications, fundraising, and any other relevant operations or initiatives.

Geographical Scope: The Privacy Framework applies to all personal information collected and processed within the boundaries of King's, operating in London Ontario, Canada. It encompasses personal information of individuals residing locally and internationally whose personal information is collected and processed by the university.

Third Parties: The Privacy Framework addresses the sharing, disclosure, and transfer of personal information to third parties. This includes service providers, contractors, vendors, affiliated institutions, government authorities, and other entities that may require access to personal information in accordance with legal requirements or for the university's operational needs. It ensures that appropriate measures are in place to protect personal information when shared with external parties.

Digital Platforms and Technologies: The Privacy Framework covers personal information collected and processed through digital platforms owned or operated by the university. This includes websites, online portals, learning management systems, mobile applications, social media platforms, and any other digital platforms utilized by the university for interacting with stakeholders or collecting personal information.

Legal and Regulatory Compliance: The Privacy Framework is designed to align with applicable privacy laws and regulations in Ontario, Canada, including but not limited to the Freedom of Information and Protection of Privacy Act (FIPPA) and the Personal Health Information Protection Act (PHIPA). It reflects King's commitment to meet its legal obligations regarding the protection of personal information.

This Scope Statement provides a clear overview of the boundaries and coverage of the Privacy Framework for King's. It sets the stage for developing comprehensive privacy policies and procedures to ensure the responsible handling of personal information and compliance with privacy laws and regulations.

1.3 Compliance

King's recognizes the critical importance of safeguarding the personal information of its students, faculty, staff, and stakeholders. Compliance with privacy laws and regulations is not only a legal requirement but also a moral and ethical responsibility.

The purpose of this section in the Privacy Framework is to emphasize the significance of complying with privacy laws and to outline King's commitment to upholding the privacy rights of individuals. It serves as a guide to ensure that King's practices align with the relevant privacy legislation in Ontario, including the Freedom of Information and Protection of Privacy Act (FIPPA) and other provincial privacy laws.

Compliance with privacy laws is essential for several reasons. Firstly, it enables King's to respect and protect the privacy rights of individuals associated with the university. By complying with privacy laws, King's establishes a framework that ensures the fair and transparent handling of personal information, fostering trust and confidence among its stakeholders.

Secondly, compliance with privacy laws helps mitigate the risks associated with privacy breaches and data mishandling. The laws provide clear guidelines on the collection, use, disclosure, retention, and disposal of personal information. By adhering to these guidelines, King's minimizes the potential for data breaches, unauthorized access, identity theft, and reputational damage.

Additionally, compliance with privacy laws strengthens King's reputation as an institution that values privacy and data protection and demonstrates King's commitment to ethical data practices, responsible information management, and respect for individual privacy rights. This commitment not only enhances King's standing among its students, faculty, staff, and alumni but also differentiates it as an organization that prioritizes privacy in an era of growing privacy concern.

To ensure compliance with privacy laws, King's has established a robust framework encompassing clear policies, procedures, and guidelines that govern the collection, use, and disclosure of personal information. It outlines mechanisms for obtaining consent, responding to privacy inquiries, managing data breaches, and addressing individual rights to access and correct personal information. In developing this Privacy Framework, King's has considered the specific requirements and obligations outlined in applicable privacy laws and regulations, including FIPPA and PHIPA. King's is committed to regularly reviewing and updating these policies and procedures to reflect changes in the legal landscape and emerging privacy best practices. By prioritizing compliance with privacy laws, King's aims to foster a privacy-conscious culture where the protection of personal information is ingrained in operations, decisions, and practices. King's commitment to compliance is rooted in its dedication to maintaining the privacy and trust of stakeholders while meeting legal obligations and ethical standards.

Definitions

2.1 Key Terminologies, Abbreviations, and Acronyms

Access and Correction Requests: Procedures for individuals to request access to their personal data held by the organization and to request corrections or updates.

Consent: Freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of their personal data.

Continuous Improvement: The ongoing process of enhancing and refining the Privacy Framework based on regular reviews, assessments, and updates.

Cross-Border Data Transfer: The movement of personal data across national borders, subject to compliance with data protection laws regarding such transfers.

Data Breach: A security incident where sensitive, protected, or confidential data is accessed, disclosed, or destroyed without authorization.

Data Controller: A natural or legal person, public authority, agency, or other body that determines the purposes and means of the processing of personal data.

Data Minimization: The practice of limiting the collection and processing of personal information to the minimum necessary for a specific purpose.

Data Processing: Any operation or set of operations performed on personal data, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, and erasure.

Data Processor: A natural or legal person, public authority, agency, or other body that processes personal data on behalf of the data controller.

Data Retention and Destruction: Policies and practices related to the length of time personal data is stored and the secure disposal of data when it is no longer needed.

Data Subject: An identified or identifiable natural person to whom the personal data relates.

Data Subject Rights: The rights afforded to individuals concerning their personal data, including the right to access, rectify, erase, restrict processing, object, and data portability.

Incident Response Plan: A documented set of procedures to follow in the event of a data breach or other privacy incident.

Personal Information: Any information relating to an identified or identifiable natural person.

Privacy Awareness Campaigns: Systematic efforts to educate and inform individuals within the organization about privacy principles, policies, and practices.

Privacy by Design: An approach to system engineering that takes privacy into account throughout the whole engineering process.

Privacy Framework Review and Updates: Processes for systematically reviewing and updating the Privacy Framework to ensure its ongoing relevance and effectiveness.

Privacy Impact Assessment (PIA): A systematic process for assessing the potential effects of a particular project or activity on the privacy of individuals.

Privacy Officer: An individual designated to oversee and ensure compliance with data protection laws and privacy policies within the organization.

Privacy Policy Statement: A formal statement that outlines an organization's practices and policies regarding the collection, use, disclosure, and protection of personal data.

Privacy Training Programs: Educational initiatives designed to inform and train personnel on privacy laws, policies, and best practices.

Stakeholders: Individuals, groups, or entities that have an interest or concern in the privacy practices and data processing activities of the organization.

Privacy Principles

3.1 Accountability

Accountability refers to an organization's responsibility for ensuring compliance with privacy laws, regulations, and internal policies regarding the handling of personal information. It entails taking ownership of personal information throughout its lifecycle and being answerable for the organization's privacy practices.

- King's assumes responsibility for the personal information it collects, uses, discloses, and retains. This includes designating individuals or teams responsible for privacy management and establishing clear lines of accountability within the organization.

- King's implements appropriate governance structures and mechanisms to oversee privacy practices. This includes developing and communicating privacy policies, procedures, and guidelines, and ensuring that they are understood and followed by all individuals involved in personal information handling.

- King's ensures compliance with applicable privacy laws, regulations, and contractual obligations. This involves understanding the legal requirements, regularly reviewing and updating privacy practices, and conducting privacy impact assessments to identify and address any potential privacy risks.

- King's provides privacy training and awareness programs to its employees and stakeholders to ensure a comprehensive understanding of privacy principles and

practices. This includes educating employees on their responsibilities and obligations related to the protection of personal information.

- King's implements appropriate technical, organizational, and administrative measures to protect personal information from unauthorized access, use, disclosure, alteration, or destruction. This includes implementing safeguards, data breach response plans, and ongoing risk assessments to mitigate privacy risks.

- King's exercises caution when sharing personal information with third parties, such as service providers or business partners. It ensures that appropriate agreements and contracts are in place to govern the handling of personal information by these parties and holds them accountable for maintaining the same level of privacy protection.

- King's demonstrates its commitment to accountability by keeping records of its privacy practices, including policies, procedures, training records, and audit trails. It may also conduct regular privacy audits or engage in third-party assessments to verify compliance and identify areas for improvement.

By adhering to the principle of Accountability, King's fosters a culture of transparency, trust, and responsibility in the handling of personal information. It ensures that privacy practices are established, monitored, and continuously improved, ultimately protecting the privacy rights of individuals and maintaining public confidence in the organization's privacy commitment.

3.2 Identifying Purposes

Identifying purpose pertains to the requirement for organizations to clearly specify and communicate the purposes for which personal information is collected, used, and disclosed. It emphasizes the importance of transparency and providing individuals with meaningful information about how their personal information will be utilized.

- King's must identify and document the specific purposes for which personal information is collected at or before the time of collection. The purposes should be defined in a clear and understandable manner, avoiding ambiguity or broad language.

- Personal information will only be collected and processed for lawful purposes that are consistent with applicable privacy laws, regulations, and contractual obligations. King's representatives and constituents must ensure that they have a legitimate basis, such as consent, contractual necessity, legal obligations, or legitimate interests, to collect and use personal information.

- Personal information will only be used or disclosed for the purposes that were identified and communicated at the time of collection, unless further consent is obtained or as required by law. King's representatives and constituents should avoid using personal information for unrelated or incompatible purposes without obtaining appropriate consent or legal authorization.

- King's will be transparent about their purposes for collecting personal information. This involves providing clear and easily accessible privacy notices or policies that outline the purposes of data collection, use, and disclosure. Individuals should be informed of any updates or changes to the identified purposes.

- Obtaining informed and voluntary consent from individuals is often necessary for the collection, use, or disclosure of personal information. King's representatives and constituents should clearly communicate the purposes to individuals and obtain their consent in a manner that is appropriate for the sensitivity of the information and the reasonable expectations of the individual.

- King's will regularly review and evaluate the purposes for which personal information is collected and used. If new purposes arise that are not compatible with the original purposes, King's should seek additional consent or assess the legal basis for the new uses.

By adhering to the principle of Identifying Purpose, King's demonstrates their commitment to respecting the privacy rights of individuals. It ensures that individuals are informed and have control over their personal information, promoting trust, transparency, and accountability in data handling practices.

3.3 Consent

Consent is based on the notion that individuals should have control and autonomy over their personal information. It emphasizes that organizations should obtain the informed and voluntary consent of individuals before collecting, using, or disclosing their personal information, except where permitted or required by law.

- King's ensures that individuals are provided with clear and understandable information about the purposes for which their personal information is being collected, used, or disclosed. Individuals should be informed of any potential risks or consequences associated with providing their consent.

- Consent should be obtained freely without any coercion or undue influence. King's representatives and constituents should avoid making consent a condition for accessing products, services, or opportunities, unless the collection of personal information is necessary for fulfilling the stated purposes.

- Individuals should have the right to withdraw their consent at any time, provided there are no legal or contractual obligations preventing them from doing so. Organizations should inform individuals of their right to withdraw consent and provide clear mechanisms for doing so.

- Where applicable and appropriate, King's should implement opt-in or opt-out mechanisms to allow individuals to express their consent or refusal to the collection, use, or disclosure of their personal information. Opt-in requires individuals to take an affirmative action to

provide consent, while opt-out presumes consent unless individuals actively indicate their refusal.

- Consent should be obtained for specific purposes. King's should not collect personal information beyond what is necessary to fulfill the identified purposes without obtaining additional consent.

- King's will take reasonable steps to ensure that individuals providing consent have the legal capacity to do so. In the case of minors or individuals lacking legal capacity, organizations should obtain consent from a parent or guardian, or as otherwise permitted by law.

- King's will maintain records of individuals' consent, including the date, time, manner of consent, and the specific purposes for which consent was obtained. These records serve as evidence of compliance and may be requested in case of disputes or regulatory audits.

Consent plays a vital role in ensuring respect for individual privacy rights and promoting trust between individuals and organizations. By adhering to the principle of Consent, King's demonstrates its commitment to ethical and responsible handling of personal information, fostering transparency, accountability, and individual control over their own data.

3.4 Limiting Collection

Limiting Collection states that organizations should limit the collection of personal information to what is necessary for the identified purposes. It emphasizes the importance of collecting only the minimum amount of personal information required to fulfill those purposes, thereby minimizing the risks associated with data breaches, unauthorized access, and potential misuse of personal information.

- King's should clearly define and communicate the purposes for which personal information is being collected. This ensures that the collection is directly related to the stated objectives and avoids unnecessary or excessive data collection.

- Personal information collected should be limited to what is necessary to fulfill the identified purposes. King's should assess the specific information needed, considering factors such as the nature of the relationship with the individual, the sensitivity of the data, and any legal or regulatory requirements.

- Personal information should only be collected with a valid legal basis, such as consent, contractual necessity, legal obligations, or legitimate interests. The collection must be lawful, fair, and compliant with applicable privacy laws and regulations.

- King's should refrain from engaging in indiscriminate or surveillance-like collection of personal information that is not directly related to the stated purposes. Collecting

information without a legitimate need or in a manner that is intrusive, or covert is not in alignment with the principle of Limiting Collection.

- King's should consider implementing data minimization techniques, such as anonymization or pseudonymization, where appropriate, to reduce the identifiability and potential risks associated with the personal information collected.

- King's should establish appropriate data retention policies and practices to ensure that personal information is retained only for as long as necessary to fulfill the identified purposes or as required by law. Retention periods should be based on legal requirements, operational needs, and the reasonable expectations of individuals.

By adhering to the principle of Limiting Collection, King's can minimize the privacy risks associated with excessive data collection and storage. This principle promotes responsible and accountable data practices, allowing individuals to have greater control over their personal information and reducing the potential for unauthorized access or misuse. Ultimately, limiting collection helps King's to maintain the privacy and trust of individuals while fulfilling their operational needs and legal obligations.

3.5 Limiting Use, Disclosure, and Retention

Limiting Use, Disclosure, and Retention emphasizes that organizations should only use, disclose, and retain personal information for the purposes for which it was collected, unless individuals provide consent or as required by law. This principle ensures that personal information is handled in a manner that respects privacy rights, minimizes risks, and promotes transparency and accountability in data practices.

- Personal information should only be used or disclosed for the specific purposes that were identified and communicated at the time of collection, unless further consent is obtained or as required or authorized by law. Organizations should not use personal information for unrelated or incompatible purposes without obtaining appropriate consent or legal authorization.

- If King's intends to use or disclose personal information for a purpose beyond the originally stated purposes, it should obtain additional consent from individuals, unless otherwise permitted by law. This ensures that individuals have control over how their information is used and disclosed.

- When sharing personal information with third parties, King's should ensure that appropriate safeguards and contractual agreements are in place to protect the privacy and security of the information. Third parties should only use the personal information for the specified purposes and in accordance with applicable privacy laws and regulations.

- King's should minimize the retention of personal information to the extent necessary to fulfill the identified purposes. Personal information should not be retained for longer than is

reasonably required, considering legal requirements, operational needs, and the individual's reasonable expectations.

- King’s should implement appropriate safeguards to protect personal information against unauthorized access, disclosure, or loss. When personal information is no longer required for the identified purposes or legal obligations, it should be securely disposed of in a manner that prevents unauthorized access or use.

- King’s should maintain records of the use, disclosure, and retention of personal information, including any consent obtained, purposes for use or disclosure, and retention periods. These records serve as evidence of compliance and accountability, supporting regulatory audits, and demonstrating adherence to privacy principles.

By adhering to the principle of Limiting Use, Disclosure, and Retention, King’s ensure that personal information is handled in a manner that respects privacy rights, reduces the potential for misuse or unauthorized access, and maintains the trust and confidence of individuals. This principle promotes responsible data practices and reinforces the organization's commitment to protecting personal information throughout its lifecycle.

3.6 Accuracy

Accuracy emphasizes the importance of ensuring that personal information collected and processed by organizations is accurate, complete, and up to date. It recognizes the rights of individuals to have their personal information maintained accurately and enables organizations to make informed decisions based on reliable data.

- King’s should take reasonable steps to ensure that personal information is accurate, complete, and relevant for the purposes for which it is collected and used. This includes verifying the accuracy of information at the time of collection and regularly updating it as necessary.

- When collecting personal information, King’s should make reasonable efforts to verify the accuracy and completeness of the data directly from the individual or from reliable sources. This helps minimize the risk of relying on incorrect or outdated information.

- King’s should provide individuals with mechanisms to review, correct, or update their personal information. This allows individuals to ensure that their information is accurate and up to date, and it enables them to exercise their rights to rectify any inaccuracies.

- King’s should strive to update personal information in a timely manner whenever new information becomes available or existing information changes. This helps maintain the relevance and accuracy of the data, particularly in situations where outdated information may have adverse consequences for individuals.

- King's should clearly communicate the importance of accuracy to individuals and inform them of their rights to review and correct their personal information. This includes providing accessible channels for individuals to request corrections or updates to their data.

- King's should establish policies and procedures for retaining personal information in a manner that ensures accuracy and relevance. Outdated or no longer necessary information should be securely disposed of or anonymized to prevent the persistence of inaccurate data.

By adhering to the principle of Accuracy, King's demonstrates its commitment to responsible data management and respect for the rights of individuals. Ensuring accurate personal information enhances the trustworthiness of the organization, enables informed decision-making, and minimizes the potential for adverse impacts on individuals resulting from inaccurate data.

3.7 Safeguards

Safeguards underscores the responsibility of organizations to implement appropriate measures to protect personal information from unauthorized access, use, disclosure, alteration, or destruction. It involves establishing and maintaining a robust security framework to safeguard personal information throughout its lifecycle.

- King's should conduct regular assessments to identify and understand the potential risks to the security and confidentiality of personal information. This includes evaluating internal and external threats, vulnerabilities, and the potential impact of a security breach.

- Based on the risk assessment, King's should implement appropriate technical, administrative, and physical safeguards to protect personal information. This may include measures such as encryption, access controls, firewalls, secure network connections, employee training, monitoring systems, and incident response procedures.

- King's should provide training and awareness programs to employees to ensure they understand their roles and responsibilities in safeguarding personal information. This includes educating employees about security best practices, data handling procedures, and the potential risks associated with mishandling personal information.

- King's should establish controls to ensure that personal information is accessed only by authorized individuals on a need-to-know basis. This involves implementing user authentication mechanisms, user access management, and monitoring of access logs to detect and prevent unauthorized access.

- King's should have procedures in place to respond promptly and effectively to data breaches or unauthorized access incidents. This includes incident reporting, containment, investigation, notification to affected individuals and regulatory authorities, and remediation measures to prevent similar incidents in the future.

- King’s should implement appropriate safeguards when sharing personal information with third parties. This includes conducting due diligence on third-party service providers, implementing contractual agreements to protect personal information, and regularly monitoring their compliance with security requirements.

- King’s should establish protocols for managing security incidents, including documenting and investigating incidents, assessing the impact, and taking appropriate measures to mitigate risks, protect affected individuals, and prevent future incidents.

By adhering to the principle of Safeguards, King’s demonstrates its commitment to protecting personal information from unauthorized access or disclosure. Implementing appropriate security measures and safeguards helps maintain the privacy and confidentiality of personal information, builds trust with individuals, and mitigates the risks associated with data breaches or unauthorized use.

3.8 Openness

Openness emphasizes the importance of organizations being transparent and open about their privacy practices and policies. It recognizes individuals' right to know how their personal information is being collected, used, disclosed, and protected, and encourages organizations to provide clear and accessible information about their privacy practices.

- King’s should develop and make available privacy policies that clearly outline their privacy practices and procedures. These policies should be written in clear and plain language, easily understandable by individuals.

- Privacy policies and related information should be readily accessible to individuals. They should be easily accessible through various channels, such as websites, mobile applications, or in-person inquiries. King’s should also ensure that individuals are aware of the existence of the privacy policies and how to access them.

- King’s should provide individuals with clear and comprehensive information about the purposes for which personal information is collected, used, disclosed, and retained. This includes details about the types of personal information collected, the entities with whom it may be shared, the rights of individuals, and any applicable consent mechanisms.

- King’s should provide individuals with privacy notices or statements at or before the time of collection of their personal information. These notices should inform individuals about the specific purposes for which their information is being collected and used.

- King’s should inform individuals of any material changes to their privacy practices or policies. They should provide updates to individuals through appropriate channels, such as email notifications, website announcements, or other communication methods.

- King’s should establish channels for individuals to ask questions, seek clarification, or voice concerns about privacy practices. This may include designated contact persons, helplines, email addresses, or online forms.

- King’s should integrate privacy considerations into their systems, processes, and practices from the outset. By implementing privacy-friendly features and practices, organizations can ensure that privacy is embedded into their operations, products, and services.

By adhering to the principle of Openness, King’s fosters transparency and trust between the institution and individuals. Openness allows individuals to make informed decisions about providing their personal information and enables them to exercise their privacy rights effectively. It also demonstrates an organization's commitment to responsible and ethical data practices and strengthens its reputation as a privacy-conscious entity.

3.9 Individual Access

Individual Access recognizes individuals' rights to access and review their own personal information held by an organization. It emphasizes the importance of providing individuals with the ability to verify the accuracy, completeness, and relevance of their personal data and to exercise control over its use and disclosure.

- King’s should inform individuals of their right to access their personal information and establish mechanisms for individuals to make access requests. This includes providing clear instructions on how to submit a request and any necessary forms or procedures.

- King’s should respond to access requests in a timely manner, typically within a specified timeframe as required by applicable privacy laws. The response should include confirmation of whether the organization holds personal information about the individual and, if so, provide access to the requested information.

- King’s should implement measures to verify the identity of individuals making access requests to ensure that personal information is only disclosed to the rightful owner. This may involve requesting specific forms of identification or using secure authentication methods.

- King’s should provide individuals with choices for accessing their personal information, such as providing copies of records, allowing individuals to view their information in person, or providing secure online portals for accessing and managing personal data.

- In some cases, King’s may charge reasonable fees for providing access to personal information. Any applicable fees should be communicated to individuals in advance, and

organizations should ensure that the fees are proportionate to the work required to fulfill the access request.

- King's may have certain limitations or exceptions on granting access to personal information. For example, access may be denied if it would infringe on the privacy rights of other individuals, if the information is subject to legal privilege, or if it could potentially harm national security or law enforcement efforts.

- If an individual identifies inaccuracies, incompleteness, or outdated information in their personal records, King's should provide mechanisms for individuals to request corrections, updates, or amendments to their personal information. This includes maintaining clear procedures for addressing and responding to such requests.

By adhering to the principle of Individual Access, King's empowers individuals to take control of their personal information and ensure its accuracy and relevance. Providing access helps build trust, enables individuals to exercise their privacy rights effectively, and demonstrates an organization's commitment to transparency and accountability in data handling practices.

3.10 Challenging Compliance

Challenging Compliance recognizes individuals' rights to challenge an organization's compliance with privacy laws, regulations, and internal privacy policies. It emphasizes the importance of providing individuals with mechanisms to voice concerns, seek redress, and seek resolution for privacy-related issues.

- King's should establish complaint mechanisms that allow individuals to raise concerns or complaints regarding the organization's compliance with privacy laws and regulations. This may include designated contact persons, helplines, email addresses, or online complaint forms.

- King's should communicate the process for submitting and handling privacy-related complaints in a clear and accessible manner. Individuals should be informed about the steps involved, the expected timeline for resolution, and any escalation procedures that may be available.

- King's should promptly and thoroughly investigate privacy-related complaints and take appropriate actions to address the concerns raised. This may involve conducting internal reviews, engaging relevant stakeholders, and implementing corrective measures to rectify any privacy breaches or non-compliance.

- King's should keep individuals informed of the progress and outcome of their complaint, providing clear explanations of the investigation findings and any remedial actions taken. Timely communication helps foster transparency and trust between the organization and the individual.

- King’s may provide alternative dispute resolution mechanisms, such as mediation or arbitration, to resolve privacy-related disputes. These mechanisms can offer an impartial and efficient means of resolving conflicts without resorting to formal legal processes.

- King’s should be aware of the role of regulatory authorities and understand the process for escalating complaints to relevant privacy oversight bodies. Individuals should be informed of their rights to file complaints with the appropriate regulatory authorities if they are not satisfied with the organization's response.

- King’s should use the feedback received through the complaint process to identify areas for improvement in their privacy practices and policies. This includes implementing measures to prevent similar issues from recurring in the future and enhancing privacy protections for individuals.

By adhering to the principle of Challenging Compliance, organizations demonstrate their commitment to accountability, transparency, and responsiveness to privacy concerns. Providing individuals with avenues to challenge compliance allows for the resolution of privacy-related issues and helps maintain trust and confidence in King’s privacy practices. It also enables King’s to continuously improve its privacy framework and enhance privacy protections for individuals.

Personal Information Collection

4.1 Types of Personal Information Collected

King’s may collect various types of personal information for administrative, academic, and operational purposes. Here is a list of potential types of personal information possibly being collected:

Basic Identification Information: Including personal details necessary to identify individuals, such as full name, date of birth, gender, and student/staff identification numbers.

Contact Information: Including addresses, phone numbers, email addresses, and emergency contact details.

Academic Information: Including records related to an individual's academic pursuits, such as program of study, courses enrolled in, grades, transcripts, academic awards, and academic performance evaluations.

Admissions Information: Including information collected during the application process, such as educational history, standardized test scores (e.g., SAT, ACT), letters of recommendation, personal statements, and admission decision letters.

Financial Information: Including information related to an individual's financial interactions with the university, such as tuition fees, scholarships, bursaries, grants, financial aid applications, and payment details.

Employment Information: Including information about individuals who are employed by the university, such as job title, department, work history, salary, tax information, and benefits.

Health Information: King's may collect health-related information for various reasons, including student health services, disability accommodations, and insurance purposes. This may include medical history, immunization records, disability documentation, and related correspondence.

Student Services Information: Including information collected by various student services departments, such as counseling, career services, student organizations, and extracurricular activities.

Library Information: King's maintains a library system that collects information on borrowed materials, overdue items, fines, and other related data.

Research Data: If individuals participate in research projects conducted by the university, their personal information may be collected as part of the research data. This can include survey responses, interview transcripts, and experimental results.

Video and Security Information: King's maintains surveillance systems in place for safety and security purposes. This may include the collection of video footage, images, and other data in public areas.

Website and Online Services Information: When individuals visit the university's website or use online services, various types of personal information may be collected, such as IP addresses, cookies, and usage analytics.

It's important to note that the specific personal information collected by King's may vary depending on its policies, practices, and legal requirements.

4.2 Collection Methods

King's may employ various methods to collect personal information from students, faculty, staff, and other individuals. Here are some possible methods of collecting personal information employed by King's:

Application Forms: When individuals apply for admission to King's, they typically fill out application forms that require personal information such as name, contact details, educational history, and relevant documentation.

Enrollment and Registration: During the enrollment process, individuals provide personal information to register for courses, select majors or programs of study, and fulfill administrative requirements. This information may be collected through online portals, registration forms, or in-person interactions.

Student Information Systems: King's, in conjunction with Western University maintains a comprehensive student information system and databases that collect and store personal

information related to students. This includes information on courses enrolled, grades, transcripts, academic history, and financial details.

Human Resources Processes: For university employees, personal information is collected through HR processes, including job applications, contracts, tax forms, and payroll records.

Online Portals and Systems: King's maintains online portals and systems for various purposes, including student services, library access, course management, and financial transactions. These systems may collect personal information through user accounts, login credentials, and activity tracking.

Surveys and Questionnaires: Universities may administer surveys or questionnaires to collect personal information for research purposes, feedback on programs or services, or institutional planning. Participation in these surveys is typically voluntary, and data is anonymized and aggregated whenever possible.

Student Support Services: Personal information may be collected by various student support services, such as counseling centers, health services, and disability offices through forms, questionnaires, and/or notes taken during sessions.

Research Projects: If individuals participate in research projects conducted by the university, personal information may be collected as part of the study. In such cases, informed consent is usually obtained, and privacy protocols are followed to protect the confidentiality of participants.

Campus Security: Universities often deploy security measures, including IP cameras, access control systems, and incident reporting mechanisms. These systems may collect personal information such as images, videos, and incident details for safety and security purposes.

External Sources: Universities may receive personal information from external sources, such as high schools, educational institutions, government agencies, or funding bodies. This information is used for admissions, scholarships, financial aid, or compliance purposes.

King's is committed to informing individuals about the purpose and methods of personal information collection and to ensure compliance with applicable privacy laws and regulations.

4.3 Legal Basis for Collection

In Ontario, Canada, the collection of personal information by King's is governed by privacy laws and regulations that establish legal bases for such collection. The primary legal basis for collecting personal information at King's includes:

Consent: Consent is a fundamental principle in privacy laws. The university must obtain the consent of individuals before collecting their personal information, unless an exception applies. Consent should be informed, voluntary, and obtained through clear and unambiguous means. King's may seek consent through consent forms, online consent mechanisms, or by providing individuals with privacy notices explaining the purposes of data collection.

Contractual Necessity: If individuals enter into a contract or agreement with the university, the collection of personal information may be necessary to fulfill the terms of the contract. For example, when students enroll in courses or employees sign employment contracts, the university may collect personal information required for administrative and operational purposes.

Legal Obligations: King's has legal obligations that require the collection of personal information. These obligations can arise from federal, provincial, or municipal laws, regulations, or government funding requirements. For example, universities may be required to collect certain information for tax purposes, immigration compliance, or reporting obligations to government agencies.

Legitimate Interests: King's may rely on their legitimate interests as a legal basis for collecting personal information. Legitimate interests refer to the reasonable and justifiable interests pursued by the university, as long as they do not outweigh the privacy rights and freedoms of individuals. Examples of legitimate interests may include maintaining campus security, conducting research, or managing administrative processes effectively.

Vital Interests: In certain situations where an individual's life, health, or safety is at risk, the collection of personal information may be justified based on vital interests. For instance, King's may collect health information or emergency contact details to ensure the well-being of students and staff in case of emergencies or medical incidents.

It's important to note that universities must comply with applicable privacy laws and regulations, such as federal, provincial or municipal legislation such as the Freedom of Information and Protection of Privacy Act (FIPPA), and the Personal Health Information Protection Act (PHIPA) in Ontario. These laws outline the legal requirements for collecting, using, and disclosing personal information, and King's must ensure they have a lawful basis for their data collection practices.

4.4 Consent Procedures

Consent procedures for collecting personal information at King's, involves ensuring that individuals are informed about the purposes of data collection, providing options for consent, and obtaining consent through clear and unambiguous means. Here are the typical steps followed in consent procedures at King's:

Privacy Notices: The university provides individuals with privacy notices or statements that explain the purposes for which personal information is collected, how it will be used, and who it may be shared with. These notices are often made available through King's websites, registration forms, or other relevant communication channels.

Clear and Understandable Language: The privacy notices and consent forms are written in clear and understandable language, avoiding technical jargon or complex legal terms. The goal is to ensure that individuals can easily comprehend the information provided and make an informed decision about granting consent.

Purpose Limitation: King's ensures that personal information is collected only for specific and legitimate purposes. The privacy notices clearly outline the purposes, such as academic administration, student support services, research, or compliance with legal obligations.

Voluntary Nature: Consent procedures emphasize that providing personal information is voluntary. Individuals should have the option to refuse or withdraw their consent without facing negative consequences, unless there are legal or contractual obligations that require the collection of certain information.

Opt-In and Opt-Out Mechanisms: King's may use opt-in and opt-out mechanisms to obtain consent. Opt-in means that individuals actively indicate their consent by checking a box or providing a clear affirmative action. Opt-out, on the other hand, means that individuals are automatically considered to have consented unless they actively indicate their objection or withdraw their consent.

Consent Forms: Consent forms may be used to obtain explicit consent for specific purposes or categories of personal information. These forms typically include information about the data being collected, how it will be used, and who it will be shared with. Consent forms may be provided in physical or electronic formats, depending on need.

Consent for Sensitive Information: If the university collects sensitive personal information, such as health information or biometric data, explicit consent may be required. Sensitive information requires a higher level of protection, and individuals must provide specific and informed consent for its collection and use.

Record-Keeping: The university maintains records of individuals' consent, including the date, time, and method of consent. This documentation helps demonstrate compliance with privacy laws and ensures accountability.

Renewal and Review: Consent may need to be periodically renewed or reviewed, particularly for long-term data collection and processing activities. King's may implement mechanisms to remind individuals about their consent status and provide options for updating or withdrawing consent.

King's ensures that their consent procedures align with applicable privacy laws.

4.5 Notification of Collection

Notification of collection procedures at King's involves informing individuals about the collection of their personal information, specifying the purposes of collection, and providing additional details about how the information will be used, disclosed, and protected. Here are the typical steps followed in notification of collection:

Privacy Notices: The university provides privacy notices or statements to individuals at the time of data collection. These notices are typically made available through King's websites, application forms, registration processes, or other communication channels. The privacy notices inform individuals that their personal information is being collected and explain the purposes for which it will be used.

Clear and Understandable Language: Privacy notices are written in clear and understandable language, avoiding technical jargon or complex legal terms. The goal is to ensure that individuals can easily comprehend the information provided and understand how their personal information will be handled.

Purpose of Collection: The privacy notices clearly specify the purposes for which personal information is being collected. This includes academic administration, student support services, research, compliance with legal obligations, or any other relevant purposes. The notice may provide examples or specific details about the types of information collected for each purpose.

Use and Disclosure: The privacy notices inform individuals about how their personal information will be used and disclosed. This includes details on who may access the information within the university, any third parties with whom it may be shared (if applicable), and the purposes for such use or disclosure. The notice may outline scenarios where disclosure is required by law or for legitimate institutional interests.

Retention and Disposal: The privacy notices may include information on how long personal information will be retained by the university and how it will be securely disposed of once it is no longer needed. This helps individuals understand the lifespan of their information within the university's systems.

Consent: Privacy notices often include information on the consent procedures and mechanisms employed by the university. This may include references to consent forms, opt-in or opt-out mechanisms, and the voluntary nature of providing personal information. The notice highlights that by continuing with the data collection process, individuals are considered to have consented to the outlined uses and disclosures unless they actively object or withdraw consent.

Security and Safeguards: The privacy notices outline the security measures and safeguards implemented by the university to protect personal information from unauthorized access, loss, or misuse. This can include information about encryption, access controls, staff training, and data breach notification processes.

Contact Information: The privacy notices provide contact details, such as a privacy office or designated individual, whom individuals can reach out to for inquiries, requests, or concerns related to the collection and handling of their personal information.

Changes and Updates: The university ensures that privacy notices are kept up to date and notifies individuals of any material changes to the collection practices or purposes. Individuals are typically provided with updated privacy notices or informed about changes through appropriate communication channels.

King’s ensures that their procedures align with applicable privacy laws.

Use and Disclosure of Personal Information

5.1 Permitted Uses of Personal Information

Permitted uses of personal information at King's refers to the authorized purposes for which the collected personal information can be used. While specific permitted uses may vary depending on the university's policies, applicable privacy laws, and the consent provided by individuals, here are some common uses within the King's environment:

Academic Administration: Personal information can be used for academic administration purposes, including enrollment, registration, course scheduling, academic advising, grading, issuing transcripts, and awarding degrees.

Student Support Services: Personal information may be utilized to provide student support services such as counseling, career guidance, disability accommodations, library services, financial aid, housing, and extracurricular activities.

Communication and Correspondence: Personal information can be used to facilitate communication between the university and individuals, including sending notifications, updates, newsletters, event invitations, and responding to inquiries or requests.

Research and Statistical Analysis: Personal information may be used for research and statistical analysis purposes, including conducting surveys, analyzing trends, performing academic research, and generating aggregated or anonymized data for institutional planning or reporting.

Campus Safety and Security: Personal information can be used to maintain campus safety and security, including monitoring access to facilities, investigating incidents, implementing emergency response protocols, and complying with legal obligations related to campus security.

Compliance with Legal Obligations: Personal information may be used to fulfill legal obligations imposed on the university, such as reporting to government agencies, complying with tax laws, responding to court orders or subpoenas, and ensuring compliance with applicable legislation and regulations.

Employment-related Purposes: Personal information of university employees may be used for employment-related purposes, including recruitment, hiring, payroll administration, benefits management, performance evaluation, and professional development opportunities.

Institutional Development and Fundraising: Personal information may be used for institutional development activities, such as alumni engagement, fundraising campaigns, donor recognition, and conducting surveys or outreach initiatives.

Accreditation and Quality Assurance: Personal information may be used to meet accreditation requirements and ensure the quality and integrity of academic programs and institutional operations.

It's important to note that the use of personal information must be in accordance with applicable privacy laws, the consent obtained from individuals, and the specific purposes outlined in the

privacy notices provided to individuals. King's will also implement appropriate safeguards to protect personal information and ensure that it is not used in unauthorized or unlawful ways.

5.2 Disclosure & Data Sharing of Personal Information

Disclosure of personal information at King's refers to the sharing or provisioning of personal information to third parties or entities outside the university. The disclosure of personal information is typically done in accordance with applicable privacy laws, the consent obtained from individuals, and the specific purposes outlined in the privacy notices provided to individuals. Here are some common scenarios for the disclosure of personal information:

Educational Partners and Service Providers: Personal information may be disclosed to educational partners, such as other educational institutions or affiliated organizations, for purposes such as credit transfers, joint programs, or collaborative research projects. Service providers contracted by the university, such as technology vendors, cloud storage providers, or mailing services, may also receive personal information as necessary to perform their services.

Government Agencies and Regulatory Bodies: Personal information may be disclosed to government agencies, regulatory bodies, or accrediting organizations as required by law or for compliance purposes. This includes sharing information for immigration compliance, tax reporting, statistical reporting, or responding to government inquiries or audits.

Research Collaborators and Sponsors: In the context of research projects, personal information may be shared with research collaborators, sponsors, or funding agencies, subject to appropriate data sharing agreements and legal obligations. This ensures compliance with ethical guidelines, promotes collaboration, and supports the advancement of knowledge.

Student Support and Health Services: Personal information may be disclosed to internal departments and professionals providing student support services, such as counseling centers, health services, accessibility services, or career development offices. This facilitates the provision of tailored support and accommodations to students.

Law Enforcement and Legal Proceedings: In certain situations, personal information may be disclosed to law enforcement authorities, such as the police or courts, in response to a subpoena, court order, or other legal requirements. This includes cooperating in investigations, addressing safety concerns, or protecting the rights and interests of individuals.

Alumni Relations and Development: Personal information may be shared with alumni associations or advancement offices for the purpose of maintaining alumni relationships, organizing alumni events, fundraising initiatives, and keeping alumni informed about university updates and achievements.

External Partners and Vendors: Personal information may be disclosed to external partners or vendors engaged by the university for specific projects, programs, or events. This includes sharing information for collaborative initiatives, conferences, or recruitment activities.

It's important to note that the disclosure of personal information will be limited to what is necessary for the specific purpose and conducted in a secure manner. King's will have appropriate data sharing agreements, confidentiality measures, and contractual arrangements in place to protect personal information when it is disclosed to third parties.

5.3 Data Transfer Outside Canada

Data transfer outside Canada from King's is subject to privacy laws and regulations. When personal information is transferred to a foreign country, the university must ensure that the recipient country provides a comparable level of protection for personal information or obtain appropriate safeguards to protect the data. Here are some key considerations for data transfer outside Canada:

Adequacy: The university may transfer personal information to a country that has been deemed by the Canadian government as having an "adequate" level of data protection. Adequacy decisions are based on an assessment of the recipient country's privacy laws and practices.

Consent: The university may obtain the informed consent of individuals for the transfer of their personal information outside Canada. The consent should clearly indicate that the information may be transferred to a foreign country and that the recipient country may have different privacy laws and standards.

Contractual Agreements: The university may enter into contractual agreements with the recipient of personal information outside Canada. These agreements may include specific clauses or provisions to protect the personal information and ensure compliance with applicable privacy laws.

Consent Withdrawal: Individuals should have the right to withdraw their consent for the transfer of personal information outside Canada at any time. The university must respect and honor such withdrawal requests.

Risk Assessment: The university should conduct a thorough risk assessment to evaluate the privacy and security implications of data transfer outside Canada. This assessment considers factors such as the nature of the personal information, the purpose of the transfer, the laws and practices of the recipient country, and the potential risks to individuals' privacy rights.

It's important for King's to assess the specific circumstances of the data transfer and seek legal advice to ensure compliance with privacy laws and regulations, particularly regarding data transfers to countries without an adequacy decision from the Canadian government.

Data Security and Retention

6.1 Safeguarding Personal Information

Safeguarding personal information is crucial for King's to protect the privacy and security of individuals' data. Implementing robust data security measures helps prevent unauthorized access, use, or disclosure of personal information. Here are King's key practices for safeguarding personal information:

Access Controls: King's will establish access controls to ensure that only authorized personnel have access to personal information. This includes user authentication mechanisms, role-based access controls, and strong password policies. Access privileges will be regularly reviewed and revoked when no longer necessary.

Data Encryption: Personal information, especially sensitive data, will be encrypted, where possible, both in transit and at rest. Encryption ensures that even if unauthorized access occurs, the data remains unreadable and unusable.

Physical Security: Physical security measures are in place to protect physical records, storage devices, and other assets containing personal information. This includes secured facilities, locked cabinets, restricted access areas, and appropriate disposal of physical records.

Data Minimization: King's will practice data minimization by collecting and retaining only the personal information necessary for the stated purposes. Unnecessary or outdated information should be securely disposed of, reducing the risk of unauthorized access or misuse.

Employee Training and Awareness: Ongoing privacy and data protection training programs will be provided to university employees. Training should cover best practices for handling personal information, the importance of safeguarding data, and the proper procedures for reporting security incidents or breaches.

Incident Response Plan: King's maintains an incident response plan in place to address security incidents or breaches effectively. The plan outlines the steps to be taken in the event of a breach, including notification of affected individuals, relevant authorities, and any required remedial actions.

Regular Security Assessments: Regular security assessments and audits are conducted to identify vulnerabilities and ensure compliance with security standards. This includes penetration testing, vulnerability scanning, and internal or external audits of data security practices.

Data Breach Notification: In the event of a data breach involving personal information, King's will promptly notify affected individuals, regulatory authorities, and any other relevant stakeholders in accordance with applicable privacy laws and regulations.

Third-Party Vendors and Contracts: When engaging third-party vendors or service providers, King's will have contractual agreements that require the vendors to maintain appropriate data security measures. This ensures that personal information shared with third parties is protected to the same standards as within the university.

Privacy by Design: The university will integrate privacy and data protection considerations from the outset when developing new systems, processes, or services. This involves incorporating privacy safeguards and data security measures into the design of IT systems, applications, and data handling practices.

By following these practices, King's can mitigate the risk of data breaches, protect personal information from unauthorized access, and ensure compliance with privacy laws and regulations.

6.2 Data Breach Response and Notification

Data breach response and notification procedures are crucial for King's to promptly and effectively address data breaches and minimize potential harm to individuals whose personal information may have been compromised. The key steps involved in King's data breach response and notification are:

Incident Identification and Assessment: The university maintains established mechanisms to detect and identify data breaches promptly. Once a potential breach is identified, it is assessed to determine the nature and scope of the incident, including the types of personal information affected and the potential risks to individuals.

Incident Containment and Mitigation: Immediate actions are taken to contain the breach and prevent further unauthorized access or disclosure of personal information. This may involve isolating affected systems, disabling compromised accounts, or implementing temporary security measures.

Investigation and Forensic Analysis: The university conducts a thorough investigation to determine the cause and extent of the breach. Forensic analysis may be performed to identify the vulnerabilities exploited, understand the impact, and gather evidence for remediation and potential legal proceedings.

Notification of Affected Individuals: If it is determined that the breach poses a significant risk of harm to individuals, the university promptly notifies affected individuals. The notification includes information about the breach, the types of personal information involved, the potential consequences, and guidance on steps individuals can take to mitigate the risks.

Communication with Authorities and Regulatory Bodies: In accordance with applicable laws and regulations, the university may notify relevant regulatory authorities, such as privacy commissioners or government agencies, about the breach. This ensures compliance with reporting requirements and allows for collaboration in investigations or enforcement actions, if necessary.

Communication with Third Parties: If the breach involves personal information shared with third parties, the university communicates with those parties to ensure they are aware of the breach and can take appropriate actions to mitigate risks or assist with the investigation.

Remediation and Incident Response Plan Updates: The university takes necessary steps to remediate the breach, address vulnerabilities, and prevent similar incidents in the future. This

may involve strengthening security measures, updating policies and procedures, and providing additional training to staff members.

Documentation and Record-Keeping: Detailed records of the breach, response actions, and communications are maintained. These records help demonstrate compliance with regulatory requirements, inform future incident response efforts, and support potential legal obligations.

It's important for King's to follow applicable privacy laws and regulations regarding breach notification, including any specific timelines or requirements outlined in those laws. By promptly responding to breaches, providing timely and accurate notifications, and taking appropriate remedial actions, King's demonstrates its commitment to protecting individuals' personal information and mitigating the potential impact of the breach.

6.3 Retention and Destruction of Personal Information

Retention and destruction of personal information is an important aspect of data management for King's. Establishing proper policies and procedures for retention and disposal helps ensure that personal information is retained only as long as necessary and is securely destroyed when it is no longer needed. King's maintains the following guidelines for retention and destruction:

Retention Policies: The university develops and maintains retention policies that specify the length of time personal information will be retained. These policies take into consideration, legal requirements, industry best practices, and the purposes for which the information was collected.

Purpose Limitation: Personal information should only be retained for the purposes outlined in the privacy notices provided to individuals. Retaining information beyond what is necessary for those purposes may pose unnecessary risks and liabilities.

Data Minimization: The principle of data minimization should be followed, meaning that only the necessary personal information required for the identified purposes should be retained. Unnecessary or redundant information should be securely disposed of.

Secure Storage: During the retention period, personal information should be stored securely to prevent unauthorized access, use, or disclosure. This includes using appropriate access controls, encryption, firewalls, and physical security measures for both digital and physical records.

Regular Review and Updates: Retention policies will be reviewed and updated regularly to ensure they align with current legal requirements and organizational needs. This may include adjusting retention periods based on changes in legislation, industry standards, or institutional requirements.

Destruction Methods: When personal information reaches the end of its retention period, it should be securely destroyed to prevent unauthorized access or unintended use. Destruction methods may include shredding physical documents, securely deleting digital files, or employing professional data destruction services.

Disposal Protocols: The university establishes clear protocols for the disposal of personal information. This includes specifying the methods, locations, and responsible parties for the destruction of physical and digital records. It's important to follow appropriate disposal procedures to ensure that personal information cannot be reconstructed or accessed after disposal.

Documentation and Record-Keeping: Records are maintained document the disposal of personal information. This includes records of the date, method, and responsible parties involved in the destruction process. Documentation supports accountability, demonstrates compliance with legal obligations, and assists in responding to any inquiries or investigations.

It's essential for King's to adhere to applicable privacy laws, regulations, and guidelines when determining retention periods and implementing secure destruction practices. By implementing robust retention and destruction processes, King's reduces the risk of unauthorized access, misuse, or retention of personal information beyond its necessary lifespan.

Access and Correction of Personal Information

7.1 Access Requests

Access requests play a crucial role in enabling individuals to exercise their rights and ensure transparency regarding the collection, use, and disclosure of their personal. King's is committed to responding to all access requests:

Access to Personal Information: Individuals have the right to request access to their own personal information held by King's. This includes information collected during the admissions process, academic records, employment-related information, or any other personal information the university may possess.

Submitting an Access Request: The university has established clear procedures for individuals to submit access requests. This includes providing access request forms, specifying contact information, and outlining the process on the King's website.

Verification of Identity: The university must verify the identity of the individual making the access request to ensure that personal information is only disclosed to the rightful owner. The verification process may involve requesting specific identification documents or employing other reasonable methods to confirm identity.

Timelines for Response: Upon receiving an access request, King's will respond within a reasonable timeframe as prescribed by privacy laws. In Canada, the general guideline is to respond to access requests within 30 days.

Providing Access: When granting access, the university will provide individuals with copies of their personal information in a commonly understandable format, unless another format is requested and is technically feasible. Access will be provided without unnecessary delay and at a reasonable cost, if any.

Exceptions and Limitations: Privacy laws may provide certain exceptions or limitations on access requests. These exceptions may include situations where access may harm the privacy of others, reveal confidential research or commercial information, or breach legal privilege. If an exception applies, the university will clearly explain the reason for denial and any recourse options available to the individual.

Redaction of Third-Party Information: If personal information includes the personal information of other individuals, the university will take steps to redact or remove that information before providing access, unless the other individuals have consented to its disclosure or its disclosure is otherwise permitted by law.

Assistance and Clarification: The university provides reasonable assistance and clarification to individuals regarding the nature and contents of their personal information, as well as the purposes for which it is used or disclosed, if necessary.

Record-Keeping: The university maintains records of access requests, including details of the request, the response provided, any redactions made, and any related correspondence. These records are important for compliance purposes and may be requested by privacy regulators or authorities.

By facilitating access requests and ensuring compliance with privacy laws, the university demonstrates its commitment to transparency and accountability in handling personal information.

7.2 Verification of Identity

Verification of identity is an essential step in the process of responding to access requests and ensuring the security and privacy of personal information. King's is committed to verifying the identity of individuals making access requests:

Requested Information: The university clearly specifies the information required for identity verification in its access request procedures. This includes details such as full name, student/employee identification number, date of birth, contact information, or any other relevant identifying information.

Secure Communication: When individuals submit access requests, King's will ensure that the communication channels used are secure. This may involve providing a dedicated email address or secure online portal for submitting requests or instructing individuals to send requests via encrypted methods.

Matching Information: The university compares the information provided in the access request with the information it already possesses for the individual. This may involve cross-referencing the details provided in the request with the individual's records, such as enrollment information, employment records, or other identifying information maintained by King's.

Verification Documents: In some cases, the university may require individuals to provide additional documentation to verify their identity. This can include a copy of a government-issued

identification document (e.g., passport, driver's license), student ID card, employee ID card, or any other document that can reasonably establish the individual's identity.

In-Person Verification: If an individual is making an access request in person, the university may ask for identification documents and compare them visually with the individual presenting them. This method helps ensure that the person making the request is the rightful owner of the personal information.

Alternative Verification Methods: In situations where individuals are unable to provide traditional forms of identification, the university may consider alternative verification methods. This could include using additional information or documents that can reasonably establish the identity of the individual, such as a utility bill, bank statement, or other official documentation.

Privacy and Data Protection: Throughout the identity verification process, the university will handle and protect the personal information provided by individuals in accordance with applicable privacy laws and regulations. This includes securely storing and disposing of any verification documents once the identity has been confirmed.

It's important for the university to strike a balance between verifying the identity of individuals and ensuring the process is convenient and accessible. The verification methods employed should be reasonable, proportionate, and in line with privacy best practices to protect individuals' personal information.

7.3 Responding to Access Requests

Responding to access requests is a critical part of ensuring transparency and respecting individuals' rights to access their personal information. King’s is committed to a timely and accurate response to all requests:

Timely Response: The university will respond to access requests within a reasonable timeframe as prescribed by privacy laws in Canada, the general guideline is to respond to access requests within 30 days. If additional time is required due to the complexity of the request or other circumstances, the individual will be notified accordingly.

Access to Personal Information: Upon verifying the identity of the requester, the university will provide access to the requested personal information. This includes providing copies of the information or allowing the individual to view the information, depending on the nature of the request and the available resources.

Format of Access: The university will provide access to personal information in a format that is commonly understandable, unless another format is requested and is technically feasible. This ensures that individuals can effectively review and comprehend the information being disclosed.

Explanation and Clarification: If necessary, the university will provide explanations and clarifications to individuals regarding the nature and contents of their personal information.

Redaction of Third-Party Information: If personal information includes the personal information of other individuals, the university will take steps to redact or remove that information before providing access, unless the other individuals have consented to its disclosure, or its disclosure is otherwise permitted by law.

Fee Considerations: King's may charge a reasonable fee for providing access to personal information if permitted by applicable privacy laws. If a fee applies, the individual will be informed in advance, and the fee will be reasonable and directly related to the costs of providing access.

Denial or Limitation of Access: In certain circumstances, privacy laws may require denial or limitation of access requests. If the university determines that access should be denied or limited based on applicable exceptions or limitations, it should clearly explain the reasons for the denial and inform the individual of any recourse options available to them.

Record-Keeping: The university maintains records of access requests, including details of the request, the response provided, any redactions made, and any related correspondence. These records are important for compliance purposes and may be requested by privacy regulators or authorities.

It's important for the university to follow applicable privacy laws and regulations when responding to access requests, ensuring that individuals' rights are respected, and their personal information is handled in a secure and transparent manner.

7.4 Correction of Personal Information

Correction of personal information is an important aspect of data accuracy and individuals' rights at King's. When individuals believe that their personal information held by the university is inaccurate, incomplete, or outdated, they have the right to request corrections. King's is committed to accurate, complete and up to date records:

Correction Requests: The university has established clear procedures for individuals to submit correction requests. This includes providing correction request forms, specifying contact information, and outlining the process on the university's website.

Verification of Identity: The university verifies the identity of the individual making the correction request to ensure that the request is coming from the rightful owner of the personal information. This helps prevent unauthorized changes or modifications.

Documentation of Correction: The individual making the correction request should provide specific details about the information they believe is incorrect, incomplete, or outdated. They should provide supporting documentation, if available, to support their claim and facilitate the correction process.

Review and Assessment: The university reviews the correction request and assesses the validity of the claim. This may involve cross-referencing the requested correction with existing records, seeking additional information or evidence, or consulting relevant sources to determine the accuracy of the information.

Making Corrections: If the university determines that a correction is necessary, we will promptly make the appropriate changes to the personal information. This may involve updating databases, records, or systems to reflect the corrected information.

Notification of Correction: The university will inform the individual of the corrections made to their personal information. This helps ensure transparency and allows individuals to verify the accuracy of the corrected information.

Communicating Corrections to Third Parties: If the university has disclosed the incorrect information to third parties, it will notify those parties of the correction, if necessary and permitted by law. This ensures that any entities relying on the corrected information can update their records accordingly.

Record-Keeping: The university maintains records of correction requests, including details of the request, the corrections made, any notifications sent to third parties, and any related correspondence. These records are important for compliance purposes and may be requested by privacy regulators or authorities.

It's important for the university to follow applicable privacy laws and regulations when processing correction requests, ensuring that individuals' rights are respected, and their personal information is accurate and up to date.

Privacy Training and Awareness

8.1 Training Programs

Training programs, in an organizational context, are designed to equip faculty, staff and other constituents with the knowledge, skills, and competencies they need to perform their roles effectively. Training is a fundamental component designed to educate and inform personnel within the organization about privacy and data protection matters. King's is committed to providing its constituents the appropriate training with the following objectives in mind.

Objectives:

a) Raising awareness of privacy and data protection principles.
b) Ensuring compliance with privacy laws and regulations.
c) Equipping personnel with the knowledge and skills to handle personal and sensitive information securely.
d) Reducing the risk of privacy incidents, breaches, and non-compliance.
e) Fostering a culture of privacy throughout the organization.

8.2 Privacy Awareness Campaigns

Privacy awareness campaigns are initiatives designed to educate and inform all individuals, including staff, faculty, students, or the public about privacy-related issues, best practices, and

the importance of protecting personal and sensitive information. These campaigns are essential in a world where data privacy and security are of increasing concern. Privacy awareness campaigns play a crucial role in creating a culture of privacy, both within King's and among the public. King's is committed to helping protect personal information, fostering trust, and demonstrating a commitment to responsible data handling by providing ongoing awareness campaigns to all its constituents.

Privacy Complaints and Inquiries

9.1 Complaint Handling Procedures

Handling privacy complaints and inquiries is a critical part of maintaining data protection and ensuring transparency for King's.

Complaint Submission:

Complaint Initiation: Individuals who wish to file a privacy complaint or make an inquiry should be provided with clear instructions on how to do so. Complaints can be submitted in writing, electronically, or through designated university channels.

Contact Information: The Privacy Office or relevant contact person should be identified for individuals to reach out to with their concerns. This information should be available on the King's website and in privacy notices.

Receipt and Acknowledgment:

Acknowledgment: Upon receiving a privacy complaint or inquiry, the King's Privacy Office or designated contact should promptly acknowledge receipt. This acknowledgment may be automated or through a personal response, depending on the preferred method of submission.

Reference Number: A unique reference number or case identifier should be assigned to each complaint or inquiry to facilitate tracking and management.

Review and Investigation:

Initial Assessment: The Privacy Office should conduct an initial assessment of the complaint or inquiry to determine its nature and validity. This involves reviewing the information provided and assessing whether it relates to a potential privacy violation or query.

Internal Notification: If the complaint or inquiry pertains to a specific department or individual within the university, the Privacy Office should notify the relevant party about the complaint or inquiry.

Investigation: For valid privacy complaints, a thorough investigation should be initiated. This may involve gathering additional information, conducting interviews, and assessing the alleged privacy breach or concern.

Resolution:

Corrective Action: If a privacy breach is identified, corrective actions should be taken promptly to address the issue. This may involve mitigating any harm, rectifying the situation, and preventing future occurrences.

Communication with Complainant: The Privacy Office should maintain ongoing communication with the complainant or inquirer, providing updates on the progress of the investigation and any remedies applied.

Documentation:

Record-Keeping: King's should maintain detailed records of privacy complaints and inquiries, including correspondence, investigation findings, actions taken, and any resolutions. These records are vital for accountability and compliance.

Response to Complainant:

Notification of Outcome: The university should inform the complainant or inquirer of the outcome of the complaint or inquiry, including any actions taken and the resolution. If the complaint is not upheld, the reasons for the decision should be provided.

Timeframe: The Privacy Office should aim to respond to privacy complaints and inquiries within a reasonable timeframe, typically within 30 days, unless an extended period is required due to complexity.

Escalation:

Internal Review: If the complainant is not satisfied with the outcome of the complaint handling process, there should be provisions for internal review. The university may assign the matter to a higher authority for reconsideration.

External Recourse:

External Privacy Regulators: If a complainant is not satisfied with the outcome of the internal process, they should be informed of their right to escalate the matter to the relevant privacy regulatory authority, such as the Office of the Privacy Commissioner of Canada.

Continuous Improvement:

Feedback and Reporting: The university should continuously monitor and assess its privacy complaint handling procedures. Feedback from complainants and inquiries should be used to improve the process and identify trends or areas where enhanced privacy measures are needed.

Transparency:

Reporting and Transparency: King's should consider disclosing information on the number and nature of privacy complaints and inquiries in its annual privacy reports, demonstrating a commitment to transparency and accountability.

These procedures ensure that privacy complaints and inquiries are addressed in a systematic and transparent manner, fostering trust among individuals whose data is processed by the university. Additionally, they help King's maintain compliance with all relevant privacy laws and regulations.

9.2 Contact Information for Privacy Inquiries

King's University College
Privacy Office
Acting Privacy Officer
Privacy@kings.uwo.ca

Privacy Framework Review and Updates

King's is committed to upholding the highest standards of privacy and data protection. As part of this commitment, King's recognizes that privacy is not a static concept but a dynamic and evolving one. To ensure the continued efficacy of its Privacy Framework, King's embraces a culture of continuous improvement through regular reviews and updates.

King's Privacy Framework is subject to systematic and periodic reviews to evaluate its relevance, effectiveness, and alignment with ever-evolving privacy laws and regulations. These reviews are conducted by a team of dedicated professionals, in collaboration with relevant stakeholders across the organization.

King's commitment to continuous improvement is exemplified in the following ways:

Regular Assessment: King's will perform annual reviews of the Privacy Framework to ensure it remains in step with the changing privacy landscape. Additional ad-hoc reviews may be

conducted in response to significant changes in privacy laws, regulations, and organizational structures.

Stakeholder Collaboration: King's recognize that the collective expertise of its stakeholders is invaluable. The review processes will involve the active engagement of the Acting Privacy Officer, the privacy team, legal and compliance teams, and other key constituents who play pivotal roles in privacy compliance.

Criteria-Driven Evaluation: During the review, King's will assess our Privacy Framework against defined criteria. This includes considering changes in privacy laws and regulations, emerging privacy risks, feedback from privacy audits, data breach incidents, and the framework's overall performance in meeting its stated objectives.

Methodical Assessment: The King's review process adheres to a systematic and structured assessment methodology. This will include assessments, interviews, audits, compliance checks, and feedback collection from relevant stakeholders to ensure a comprehensive evaluation.

Transparency and Accountability: King's maintains detailed documentation of review findings, conclusions, and recommendations. A formal review report will be created and shared with relevant stakeholders and decision-makers, ensuring transparency and accountability in our processes.

In addition to King's review efforts, the university has established a robust framework for framework updates. This involves systematic change management, engagement with relevant stakeholders, development of detailed implementation plans, clear communication strategies, comprehensive training and awareness campaigns, and diligent documentation and record-keeping.

King's dedication to continuous improvement is driven by its commitment to safeguarding the privacy of individuals and maintaining compliance with privacy laws and regulations. King's understands that privacy is a fundamental right, and the Privacy Framework will continue to evolve to meet the challenges of a changing world. Through these ongoing efforts, King's aims to reinforce trust and confidence in its privacy practices while staying responsive to the evolving landscape of privacy and data protection.

Appendices

11.1 Privacy Policy Statement

King's, is committed to protecting your privacy and ensuring the security of your personal information. This Privacy Policy Statement outlines King's practices and policies regarding the collection, use, disclosure, and protection of your personal data. King's adheres to the highest standards of privacy and data protection and are dedicated to complying with all applicable privacy laws and regulations.

Our Commitment to Privacy:

1. Transparency: King's is committed to being transparent about its data collection and processing practices. King's will inform you about the type of information it collects, how it is used, and who it may be shared with.
2. Data Minimization: King's will only collect and process data necessary for legitimate purposes. King's does not collect more data than is required.
3. Consent: King's will seek your explicit consent before collecting and processing your personal information whenever required by law.
4. Security: King's has implemented rigorous security measures to protect your data from unauthorized access, disclosure, alteration, or destruction. Your data is treated with the highest level of security.
5. Access and Control: King's will provide you with options and mechanisms to access and control your personal information. You have the right to review, update, and delete your data.
6. Data Retention: King's retains your personal data only for as long as it is necessary to fulfill the purposes for which it was collected and to comply with legal requirements.
7. Data Sharing: King's may share your data with trusted partners and service providers when necessary. King's ensures that they also uphold stringent data protection standards.
8. Cross-Border Data Transfer: If King's transfers your data across international borders, we will take all necessary measures to protect it and ensure compliance with applicable laws.

Your Rights:

You have the right to:

- Know what personal information King's holds about you.
- Access your data and request corrections.
- Withdraw your consent for data processing.
- Request data deletion in certain circumstances.
- Object to King's data processing practices.

Contact Us:

If you have any questions, concerns, or requests related to your privacy or this Privacy Policy, please contact King's Acting Privacy Officer at:

King's University College
Privacy Office
Acting Privacy Officer
Privacy@kings.uwo.ca

King's takes your privacy seriously and are committed to addressing any inquiries or concerns promptly and effectively.

Effective Date:

This Privacy Policy Statement is effective as of [Effective Date]. Any updates or revisions will be communicated through King's official channels.

11.2 Consent Forms

11.2.1 Agreement for the Confidentiality and Security of Personal Information

AGREEMENT for the CONFIDENTIALITY AND SECURITY OF PERSONAL INFORMATION and/or

CONFIDENTIAL BUSINESS DATA

Between

King's University College

and

[insert name of the Company] (The Company)

WHEREAS King's University College wishes the Company to provide, and the Company wishes to provide the services more fully set out in [insert the agreement or P.O. number applicable];

AND WHEREAS such services will require the Company to have access to and/or possession of and/or use of personal information and/or confidential business data under the control of King's University College, they shall be subject to the terms and conditions hereinafter set out;

NOW THEREFORE in consideration of the mutual covenants, agreements and undertakings herein contained, the Company on behalf of itself and its successors and assigns and King's University College on behalf of itself and its successors mutually covenant and agree as follows:

1. TERM. The term of this agreement shall be the period for which the Company is providing services to King's University College that require the Company to have access to and/or possession of and/or use of personal information and/or confidential business data under the control of King's University College.

2. PERSONAL INFORMATION. The Parties recognize the application of the Municipal Freedom of Information and Protection of Privacy Act, R.S.O., 1990, c.M-56 (MFOI/POP) and Regulations thereunder, as amended from time to time, to the collection, use and disclosure of personal information under the control of King's University College.

    a. For the purpose of the application of the MFOI/POP, the definition of personal information shall be as defined pursuant to MFOI/POP.

3. COLLECTION BY COMPANY. The Parties recognize the application of the Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31 (FIPPA) and Regulations thereunder, as amended from time to time, to the collection, use and disclosure of personal information by the Company for its own use and/or benefit.

    a. For the purpose of the application of FIPPA, the definition of personal information shall be as defined pursuant to FIPPA.

    b. The Parties agree that at no time will the Company for its own use and/or benefit collect, use and/or disclose personal information about and/or belonging to applicant, students, faculty, staff, or alumni of King's University College.

3. WARRANTIES AND COVENANTS. Without limitation to any other provision of this Agreement, the Company represents and warrants to and covenants with King's University College as follows, at all times during which the Company is providing services that may require the Company to have access to and/or possession of and/or use of personal information and/or confidential business data under the control of King's University College:

    a. the Company shall comply with all provisions of MFOI/POP and all King's University College's policies and procedures regarding the collection, use and disclosure of personal information and/or confidential business data under the control of King's University College;

    b. under no circumstances shall the Company or its employees disclose personal information and/or confidential business data under the control of King's University College;

    c. the Company shall employ appropriate security measures, as determined by King's University College, in its sole discretion, to protect the confidentiality of the personal information and/or confidential business data in its possession but under the control of King's University College if in the Company's possession as a result of the services being provided for King's University College;

    d. only those employees or agents employed by the Company who require access to personal information and/or confidential business data under the control of King's University College for the purpose of performing their duties with respect to the services being provided to King's University College shall be provided with access to such personal information;

    e. the Company shall either return or destroy, as determined by and in a manner to be determined by King's University College in its sole discretion, any and all personal information and/or confidential business data under the control of King's University College if in the Company's possession as a result of the services provided by the Company to King's University College;

    f. the Company, except as may be required by law, agrees to not use, directly or indirectly, for its own account or for the account of any person, firm, or

other entity or disclose to any person, firm, or other entity, King's University College's confidential business data disclosed or entrusted to it or developed or generated by it in the performance of its duties hereunder, including but not limited to information relating to King's University College's organizational structure, operations, business plans, technical projects, business costs, research data results, inventions, trade secrets, or other work produced, developed by or for King's University College, whether on the premises of King's University College or elsewhere. The foregoing provisions shall not apply to any proprietary, confidential or secret business information which is, at the commencement of the Term or at some later date, publicly known under circumstances involving no breach of this Agreement or as lawfully and in good faith made available to the Company without restrictions as to disclosure to a third party; and

g. the Company shall at all times indemnify and save harmless King's University College, its directors, trustees, members, officers, employees, agents, successors and assigns from and against any and all claims, demands, liabilities, losses, costs, damages, actions and causes of action by whomsoever made, sustained, brought or prosecuted in any manner based upon, occasioned by or attributable to anything done or omitted to be done by the Company, its directors, officers, employees, agents, authorized assigns or sub-contractors of the Company including negligent acts or negligent omissions in connection with duties set out above and performed, purportedly performed or required to be performed by the Company under this Agreement and including any breach of its obligations contained herein.

4. SURVIVAL. All representations, covenants, warranties, indemnities and limitations of liability set out in this agreement shall survive the termination or expiry of this agreement.
   IN WITNESS WHEREOF the parties hereto have caused this Agreement to be signed by their duly authorized officers as of the date first below written.

On Behalf of
[insert name]

_____
date

_____
signature

On Behalf of the Company, [name]

Title [insert]
Individual [insert name]

_____
signature

11.3 Privacy Impact Assessments (PIA)

A Privacy Impact Assessment (PIA) is a systematic process used to identify and assess the privacy implications of a project or system. The assessment helps ensure that privacy risks are identified and appropriately managed, in compliance with relevant privacy laws and regulations.

A PIA is typically necessary in situations where King's, is planning to implement a new project, system, or process that involves the collection, use, or handling of personal information. The goal of a PIA is to identify and assess potential privacy risks associated with the project and to develop strategies to mitigate or manage those risks. Here are some common scenarios where a PIA may be necessary:

1. Introduction of New Systems or Technologies: When King's is planning to implement new information systems, databases, or technologies that involve the processing of personal data, a PIA is often necessary. This could include new student information systems, learning management systems, or any other technology that deals with sensitive information.
2. Changes to Existing Processes: If there are significant changes to existing processes that involve the handling of personal information, such as changes to data storage, data sharing practices, or data retention periods, a PIA may be required.
3. Third-Party Relationships: If King's is entering into partnerships or contracts with third-party vendors or service providers that will have access to personal information, a PIA may be necessary to assess and manage the privacy implications of these relationships.
4. Research Projects: In the case of research projects involving the collection or processing of personal data, especially sensitive data, a PIA may be required to ensure that privacy considerations are adequately addressed.
5. Legislative or Regulatory Requirements: Some jurisdictions or regulatory bodies may require King's to conduct PIAs for certain types of projects or data processing activities to ensure compliance with privacy laws and regulations.

Responsibilities of the initiating business unit or faculty:

Once a business unit or faculty have determined that their project should have a privacy impact assessment, the project lead should complete the preliminary privacy analysis questionnaire and send it to the Privacy Office. The Privacy Office will review the information, and confirm whether a PIA is necessary. PIAs are led by the Privacy Office and often involves collaboration with relevant partners in the Information Security Office, the Software and Technology Assessment Panel (STAP) and possibly outside legal services. Project leads work with the Privacy Office to provide information regarding how personal information fits into the project, and to provide compliance with guidance on best practices. Vendors are also often involved in providing additional information about their privacy and security practices through a STAP provided questionnaire.

1. Begin the Privacy Impact Assessment (PIA) process early in the project timeline to allow for meaningful integration of potential changes. Depending on the complexity of the services or project, the completion of a PIA may take up to one month.
2. Once the PIA process is initiated, the Privacy Office will guide you through more detailed steps in completing the assessment.
3. Furnish the Privacy Office with ample information to facilitate a thorough analysis.
4. Act upon any recommendations outlined in the PIA final report.
5. If there are significant alterations to the project plan, re-initiate the PIA process. The iterative nature of the PIA ensures that impacts on privacy compliance are effectively addressed.
6. Continuously monitor the project for risks and, if necessary, consult with the Privacy Office.

NOTE: For a copy of the preliminary privacy analysis questionnaire, contact the Privacy Office.

11.5 Privacy Framework Approval

Ongoing Commitment:

King's University College is committed to upholding the principles and practices outlined in this Privacy Framework. This commitment extends to all Faculty, Staff, contractors and constituents who handle personal and sensitive information on behalf of the organization.

Acknowledgment:

By their approval, [Name and Title of the Highest Executive Officer] and King's University College acknowledge the importance of protecting the privacy of individuals and commit to fostering a culture of privacy throughout the organization.

On Behalf of

King's University College

_____

date

_____

signature