ECC

European City Campus

EUROPEAN CITY CAMPUS (PVT) LTD

GENERAL POLICIES

Student Protection Policy

Section 1: Document Content

1. A Student Protection Plan is an official document that outlines the steps European City Campus (ECC) will take in circumstances jeopardizing students' educational pursuits. As a recognized higher education provider, ECC is obligated to maintain this document to communicate how it will ensure students' well-being.

2. In the event of situations requiring the Student Protection Plan, ECC will:

a. Maintain transparency about the likelihood of such situations.
b. Notify the Student Coordinator.
c. Collaborate with affected students to understand how proposed changes may impact them and identify solutions.
d. Thoroughly assess the impact on affected students, considering their concerns.
e. Strive to facilitate students' continuity of studies within ECC or with an alternative provider.
f. Provide refunds or compensation if ECC cannot find a suitable solution, directing refunds to the original payer.

Section 2: Risk Mitigation Plan

1. ECC's Executive Board and Board of Management manage institutional aspects through a risk-based approach, evaluating risks in a central registry. ECC's forward-thinking approach aligns with the 2028 strategic plan, formulating an annual plan to anticipate, mitigate, and monitor risks.

2. ECC has a comprehensive business continuity strategy, regularly disclosing financial performance and risk information to regulatory bodies for compliance.

3. Strategic plans, risk registers, and business continuity plans undergo periodic reviews, with student representatives playing a vital role in decision-making and continuous risk monitoring.

Question 1: ECC Dissolution or Degree Issuance Loss

1. ECC does not anticipate closure or loss of degree-awarding authority. In the unlikely event, efforts will be made to enable students to complete their studies, offering alternatives and necessary certifications.

Question 2: ECC Closure or Relocation

1. ECC has no intention to close, but in emergencies or relocations, measures will minimize disruptions. Consultations with students will occur, and additional expenses will be addressed case by case.

Question 3: Course or Delivery Mode Discontinuation

1. Periodic assessments may lead to course discontinuation, with affected students provided alternatives and exit awards. Decisions will be made in advance to mitigate impacts on applicants.

Question 4: Course Significant Changes

1. Regular course reviews occur, and significant changes follow a process similar to course discontinuation.

Question 5: Government Emergency Restrictions

1. Protocols ensure education continuity during government-imposed restrictions, with policies developed in collaboration with students.

Question 6: Professional Accreditation Loss

1. In case of accreditation loss, ECC engages with students, addresses reasons, and communicates until reinstatement.

Question 7: TVEC License Revocation

1. ECC monitors TVEC accreditation, and in rare cases of revocation, students may continue studies or explore alternatives.

Question 8: Strike or Staff Absence

1. ECC minimizes disruptions during staff absence through alternative learning opportunities or suitable replacements.

Question 9: Critical Study Services Unavailability

1. ECC's business continuity plan ensures access to necessary services in alternative locations, with individualized support for additional costs.

Question 10: Students at ECC Collaborating Partners

1. Students at partner universities are treated like ECC students, receiving protection and support equivalent to ECC's own students.

Data Protection Policy

This policy concerns the protection of personal information, encompassing any data that can identify an individual, whether directly or when combined with other available data. Certain types of personal data, termed special category data, are particularly sensitive and demand utmost caution in handling. This includes details regarding race, ethnicity, religion, medical records, political affiliations, genetic or biometric information, among others. For detailed instructions on managing this special category data, please consult our Sensitive Data Policy. Adherence to this policy is mandatory for both employees and students at the European City Campus (ECC), and failure to comply may lead to disciplinary measures. Data protection laws also impose obligations when handling personal data on devices not controlled by ECC, like through instant messaging services, where data protection regulations must be followed.

In case of a data breach or suspicion of one, it's crucial for employees and students to promptly reach out to the Data Protection Officer at DPO@europeancitycampus.lk. Additionally, ECC's Data Protection Committee provides tools and support via dedicated intranet sites to assist Schools and Services in complying with information legislation.

Scope

This policy pertains to both individuals and organizations that handle ECC's personal data. It covers a broad spectrum of activities involving such data, such as identifying, gathering, recording, organizing, storing, altering, accessing, using, sharing, restricting, deleting, or disposing of it.

Moreover, this policy encompasses the electronic handling of personal data, including via email, word processing documents, software programs, and manual files specifically designed for easy access to personal information.

Data Collection and Processing Objectives

To fulfill its crucial operations, ECC needs to gather and store different types of personal and sensitive data regarding its staff, students, and other users of ECC facilities. To meet legal obligations, ECC and any party handling personal data for ECC must:

1. Establish and apply controls, both technical and organizational, to show compliance with data protection principles.
2. Empower individuals to exercise their Information Rights and adhere to authorized codes of conduct for data protection.
3. Use personal data exclusively for explicitly outlined and specified purposes.
4. Keep personal data for a duration that is reasonably essential.

Data Protection Principles

When dealing with personal data, certain principles should guide its handling, including collection, usage, retention, transfer, disclosure, and destruction. The Data Protection Committee's Intranet site provides further guidance on these principles:

1. Legality, Fairness, and Transparency: Personal data processing must be lawful, fair, and transparent.
2. Purpose Limitation: Collect personal data only for specific, clear, and legitimate purposes without using it for incompatible objectives.
3. Data Minimization: Gather only necessary, relevant, and adequate personal data for the intended purpose.
4. Accuracy: Maintain accurate and updated personal data as needed.
5. Storage Limitation: Store personal data for identification purposes only as long as necessary.
6. Integrity and Confidentiality: Process personal data securely to prevent unauthorized access, loss, or damage.
7. Accountability: Comply with the law by documenting processes, procedures, and policies.

Responsibilities

At the senior management tier, the Executive Board has assigned the Chair of the Data Protection Committee (CDPC) the duty of overseeing personal data security. The CDPC holds independent authority and bears ultimate responsibility for ensuring ECC meets its data protection obligations. Specifically mandated by the General Data Protection Regulation, the CDPC operates independently and reports directly to the highest echelon of organizational management. Moreover, the CDPC acts as the primary point of contact for both Supervisory Authorities and individuals whose data is under management.

Each Department Head is tasked with advancing and modeling optimal data protection standards within their teams. They are also required to inform the CDPC of any alterations in the gathering, utilization, and security protocols related to personal data processing within their specific departments. To further support this, the Information Assurance Office will train ECC personnel to function as Data Protection Advisors. These individuals will promote best practices and raise concerns regarding data protection within their respective departments. The responsibilities concerning data protection extend across all levels of the organization, encompassing senior management, employees, and students.

Information Rights

Each person whose personal information is handled by ECC holds specific entitlements concerning the usage and control of their data. ECC commits to evaluating all inquiries regarding information rights in accordance with relevant laws and rules. Those handling personal data for ECC are required to work alongside the Information Assurance Office to meet their responsibilities in addressing requests related to information rights.

Remote Work

The guidelines and rules outlined in the Personal Data Protection Act, No. 9 of 2022, are still relevant during remote work. All staff members have a responsibility to ensure the protection and separation of any data they handle while working from home, even if they're using personal gadgets or physical documents. Certain software like Office 365 is safeguarded through security measures like multi-factor authentication, data encryption, and potential limits on downloading and sharing. When using personal devices, employees need to maintain updated software and have antivirus programs installed. Communication involving data should occur through ECC email, Microsoft Teams, OneDrive, or SharePoint accounts. It's strictly prohibited to share ECC-related data through personal email, personal cloud storage, or other communication platforms.

Software and Hardware Recommendations

IT Services at ECC are responsible for providing and supporting a range of systems, applications, and services crucial to ECC's operations. These systems undergo evaluations to ensure they meet specific requirements related to functionality, data storage, disaster recovery, security, and regulatory compliance, particularly with laws concerning data protection.

Individuals at ECC who wish to use applications, software, or services not recommended by IT Services must establish controls to ensure ECC remains compliant with the Data Protection Act and other pertinent laws. Due to the intricacies of compliance, seeking guidance from IT Services before adopting new systems, apps, or services is highly encouraged. The Information Assurance Office can aid in assessing compliance when needed, but prior notification is necessary for evaluating unsupported applications, systems, or services.

Should the use of an unsupported system, application, or service pose risks to ECC, the CDPC or a designated representative will outline these risks and suggest potential measures for mitigation. If these recommended measures are not implemented and the risk is accepted, the Information Assurance Office will seek approval for these risks via a Risk Approval Form signed by the relevant Head or Director of Service, subject to periodic review.

In cases where such systems, applications, or services could compromise data protection obligations, the CDPC is legally obligated to notify the relevant Heads or Directors, and if necessary, the Executive Board. Violations of data protection principles mandate ECC to cease processing personal data that breaches the law, and the Information Assurance Office will take urgent measures to ensure compliance.

Requests and Disclosures from Law Enforcement

In specific situations, personal information might be revealed without the individual's awareness or approval. These instances encompass scenarios like preventing or identifying crimes, capturing or taking legal action against wrongdoers, gathering taxes or fees, or as mandated by a court order or legal regulations. Should ECC or an authorized third party handle personal data for these reasons, they can bypass the usual limitations outlined in this policy, but solely to the extent required. Should an ECC staff member receive a demand for personal data from a court or law enforcement entity, they must pass it on to the Data Protection Officer, who will offer thorough direction and assistance.

Data Security Training

All individuals affiliated with ECC, including employees, contractors, temporary workers, and volunteers granted access to personal data, are educated about their obligations as outlined in this policy during their onboarding through comprehensive staff induction training. This training encompasses data protection principles. Specialized data protection training is tailored for departments dealing extensively with personal or sensitive data. A dedicated data protection intranet site is accessible to all ECC employees and students, offering essential guidelines and resources facilitating adherence to data protection protocols.

Transfers and Sharing of Data

ECC has the possibility to reveal or move personal information, including special category data, to internal recipients or other entities (Data Processors) for the purpose of delivering services on its behalf. ECC and its affiliated entities will only transfer or share personal data with third parties or provide them access if they are confident that the recipient and/or data processor will handle the information in a legal and accountable manner.

Handling of Complaints

People wanting to raise concerns about how their personal information is handled should start by putting their complaint in writing to the Data Protection Committee. Each complaint will be looked into individually, and if needed, an inquiry will be carried out. The Data Protection Committee or a chosen representative will keep the complainant updated on how the complaint is progressing and when it’s resolved, within a reasonable amount of time.

Breach Notification

Anyone who suspects that personal data has been compromised through theft, loss, or exposure is required to promptly contact the Data Protection Officer Committee. They should provide a detailed description of the incident. Reports can be submitted via email to DPO@europeancitycampus.lk. Upon receipt, the DPO or an authorized representative will investigate the reported incidents to determine if a breach of personal data has indeed occurred. If confirmed, the Data Protection Committee (DPC) will take appropriate legal actions based on the scale and nature of the compromised personal data. In cases of severe breaches, the DPC will mobilize an emergency response team to manage the situation and, if necessary, notify the relevant Supervisory Authority.

Data Retention

Specific kinds of data need to be kept for extended durations because of legal, financial, archival, or other business requirements. ECC will eliminate personal information that has ceased to be necessary, following the storage limitation principle. To set consistent retention periods for commonly gathered data, a Records Retention Schedule has been developed.

CCTV

ECC administers closed-circuit television (CCTV) setups across its campuses, incorporating stationary cameras for multiple objectives. These objectives encompass safeguarding ECC staff, students, guests, and property, preventing and identifying unlawful activities, and overseeing site security. These systems align with ECC's disciplinary protocols and hold the potential for apprehending and pursuing legal action against perpetrators. Moreover, footage from these systems might be utilized as evidence in both criminal and civil proceedings.

Network and Account Monitoring

ECC utilizes preemptive strategies to safeguard personal data, technology, infrastructure, computer networks, and intellectual assets. Each network user possesses a distinct username and password for their account, enabling IT Services to monitor activities recorded within those accounts, such as website visits, email correspondence, and instant messaging. To reduce the likelihood of personal data exiting the network via Office 365 channels, Data Loss Prevention technology is deployed. Additionally, the Data Protection Committee investigates any instances of such actions reported to ensure adherence to information regulations.

Offenses Against Data Protection

Unauthorized access, sharing, or selling of personal data from ECC systems violates the Data Protection Act. It's also prohibited to hold onto this data beyond job requirements or after leaving employment without ECC's permission. Altering, deleting, or hiding personal data to avoid lawful disclosure, or thoughtlessly re-identifying de-identified data without ECC's consent, is not allowed. Breaches of the Personal Data Protection Act, No. 9 of 2022, will undergo disciplinary scrutiny, potentially resulting in dismissal or expulsion upon confirmation of an offense.

Equality, Diversity & Inclusion Policy

Introduction:

The European City Campus (ECC) is dedicated to a comprehensive overhaul of its curriculum, teaching methods, research impact, and collaborative initiatives to bolster the achievement of its students, graduates, and the broader community. The primary goal is to establish ECC as Sri Lanka's leading university, emphasizing career-focused education and entrepreneurship. The aim is to equip students for future professional paths while fostering sustainable innovation in an inclusive manner.

For ECC to realize this ambition, it must prioritize equity, diversity, and inclusion, not solely within student services but also as an employer. This involves recruiting and nurturing staff members who possess the expertise and commitment needed to nurture and sustain a work culture that champions equality and inclusion, while steadfastly opposing discrimination and exclusionary conduct.

The central objective is to fashion a workplace that is inclusive, fair-minded, and respectful—where each person is esteemed, empowered to achieve their utmost potential, and actively contributes to the organization's triumph.

Policy Statement:

ECC is dedicated to promoting inclusion within its diverse community, aiming to ensure fairness and parity in the experiences of both staff and students. The primary goal is to establish ECC as an exceptionally inclusive higher education institution in Sri Lanka, aligning with its strategic vision. This entails embracing the diversity within the community, valuing its enriching aspects, and actively combating discrimination—be it sexism, racism, ableism, homophobia, transphobia, anti-Semitism, Islamophobia, or any other form of bias that marginalizes individuals. ECC recognizes the interconnectedness of these characteristics within individual lived experiences.

Creating an inclusive environment that fosters a sense of belonging and encourages meaningful contributions requires a commitment to free speech, academic freedom, and the elimination of hate speech. Prioritizing psychological safety is essential to facilitate respectful discussions, even when differing opinions arise. This ongoing and evolving process demands active engagement from all stakeholders.

This document outlines ECC's policy on Equality, Diversity, and Inclusion (EDI), serving as a catalyst for the aforementioned goals and interconnected with other relevant institutional policies.

Institutional Context:

ECC's approach to Equity, Diversity, and Inclusion (EDI) is steered by values like inclusivity, bravery, and enthusiasm. The strategy's goal is to expedite the growth of diverse talent in any area it's found, positioning ECC as the top preference for employers, innovators, and those adept at tackling challenges. ECC is dedicated to maintaining a reputation for providing outstanding education, fostering learning, and ensuring fair outcomes for all students.

To track advancements, ECC has set Key Performance Indicators (KPIs) intricately tied to equality and diversity, aligning with the diverse makeup of ECC's community.

Scope:

This guideline applies to all individuals within the ECC community, spanning from the Executive Board and employees to students, visitors, contractors, subcontractors, and service providers involved in the institute's activities across its locations.

Its aim is to establish a structure that incorporates Equality, Diversity, and Inclusion (EDI) principles throughout ECC's operations and services. Due to its extensive scope, this structure is interconnected with various other plans and programs. Each specific strategy and policy will carry its own set of objectives and actions. Additionally, there will be a dedicated Equality Action Plan regularly updated to serve as a central guide for identifying and overseeing EDI initiatives linked to functions impacting both staff and students.

Responsibilities:

While it is expected that all members of the ECC community uphold values of inclusivity, respect, and fairness, the primary responsibility for ensuring these principles lie with the Chairman, Executive Board, and Board of Management in their day-to-day operations.

The Ethics and Advisory Committee will oversee matters concerning Equity, Diversity, and Inclusion (EDI) and guide the ECC Ethics and Advisory Committee in implementation. This committee will supervise operations, align EDI policies, drive action plans, and accelerate progress towards institution-wide EDI goals, including Gender and Race Equality.

The Board of Management is tasked with executing this EDI policy, identifying local diversity challenges, and creating initiatives tailored to address these issues, especially those impacting academic performance.

All employees and students are obliged to align their conduct with this Policy, as compliance is a fundamental expectation within their contractual relationship with ECC. This requires understanding the policy, committing to behavior that reflects it, acknowledging the benefits of nurturing an inclusive culture, and actively engaging in learning opportunities and available resources. Breaches of behavioral standards may lead to ECC's regulations governing conduct and capabilities.

The Ethics and Advisory Committee will aid in formulating and overseeing this policy in collaboration with the Executive Board. The Executive Board holds the responsibility of spearheading new initiatives that foster diversity, authentic equal opportunities, and the elimination of barriers to equality. Collaboration with faculty and students is integral to achieving EDI objectives.

Principles of Implementation:

This Policy aligns with various specific policies and strategies, each outlining action plans to achieve strategic and policy objectives. The implementation of this policy is guided by key principles to ensure a unified and consistent approach:

- Evidence-centered approach: The policy will be founded on thorough research and engagement with stakeholders.

- Blend of quantitative and qualitative data: Utilizing both quantitative and qualitative equality and diversity data, ECC will compare internal data with external benchmarks when possible. The process will involve comprehensive consultations, including Race Equality self-assessment procedures. Data dashboards will aid in monitoring progress for both staff and students, guiding the identification of future initiatives.

- Diverse sources of evidence: Data sources will encompass staff and student demographic information, staff survey feedback, institutional self-assessment findings (Race Equality), collaborations with specialized EDI teams, and broader EDI strategy surveys and focus groups.

Definitions:

- Equality at ECC centers on adhering to the Equality Act 2010 and preventing discrimination through policies, ensuring equal opportunities regardless of background, beliefs, disabilities, age, sexual orientation, or gender identity.

- Discrimination happens when someone is treated unfavorably due to a protected characteristic they possess or are associated with. It can occur openly or through practices that disproportionately disadvantage certain groups, unless justifiable.

- Associational Discrimination involves direct discrimination against someone because of their association with a person having a protected characteristic.

- Perception Discrimination refers to direct discrimination against someone perceived to possess a protected characteristic.

- Victimization occurs when someone faces unfair treatment for raising or supporting a discrimination complaint.

- Diversity efforts at ECC aim to create a staff community mirroring the local demographics while acknowledging individual uniqueness.

- Inclusion embodies ECC's dedication to accepting everyone, providing equal access, eliminating prejudice, and fostering an inclusive environment.

- Bullying related to sexual orientation or gender identity involves targeted abuse against individuals perceived as LGBTQ+, including derogatory remarks or outing without consent.

- Bullying against Trans individuals includes intentional use of incorrect pronouns or past names. Bi-specific bullying negates a person's identity based on their sexual orientation.

- Racism covers discrimination based on skin color, nationality, ethnicity, or national origin. It encompasses individual, institutional, and structural forms, affecting experiences and outcomes within society and institutions.

Ethical Framework

Vision:

We aim to become a prominent academic institution known for its exceptional standards, propelled by continuous innovative approaches.

Mission:

Our goal is to offer an empowering education that enables people to achieve their utmost and make positive contributions to society. Through innovative programs, we aim to foster critical thinking and a lasting enthusiasm for learning. Alongside this, our research tackles significant societal issues and pushes the boundaries of knowledge. We're devoted to readying our students to be conscientious global citizens, promoting teamwork, diversity, and ethical guidance. Ultimately, our aim is to shape individuals into ethical leaders, catalysts for change, and perpetual learners, leaving a meaningful, positive mark on the world.

Core Values:

The core values and atmosphere at European City Campus (ECC) revolve around ethical ideals such as fairness, equality, conscientiousness, and valuing individuals' rights. These principles are showcased through our dedication to trustworthiness, truthfulness, uprightness, mutual support, regard for others, being open to fresh perspectives, fostering creativity and groundbreaking thinking, striving for top-notch standards, encouraging personal development, teamwork, clear communication, being responsible and answerable, and recognizing accomplishments. Additionally, we prioritize contributing to both our campus and the wider community through our emphasis on service.

Management & Leadership Values:

We lead with a forward-thinking and motivating strategy, fostering a common vision, and maintaining ethical and fair management principles.

Teaching & Learning Values:

The faculty at European City Campus are committed to delivering top-notch education by customizing learning to suit each person's goals, embracing growth-oriented teaching methods, catering to various learning preferences, nurturing independent and thoughtful learners, considering students' overall development, setting ambitious standards for achievement, utilizing technology efficiently, encouraging collaboration across subjects, and embodying the values ingrained in the curriculum. Additionally, we prioritize giving consistent feedback to both students and teachers to aid in the learning journey.

Core Ethical Principles:

As ECC strives for its vision, it remains dedicated to a core set of principles deeply rooted in basic moral values. These encompass honoring the innate humanity, individuality, dignity, and diverse cultures of others, upholding freedom of expression, ideas, and academic exploration within lawful boundaries, enabling all faculty and students to achieve their utmost capabilities, and conscientiously addressing environmental, social obligations, and sustainable progress.

Commitment to Equality, Diversity, and Inclusion (EDI):

Our plan emphasizes our dedication to nurturing an authentically inclusive atmosphere where everyone has fair chances for success, and where we celebrate and encourage the diversity within the ECC community to thrive.

Activities:

Our approach corresponds with ECC's Vision, Mission, and Values through a range of endeavors. These include readying upcoming graduates, advancing communities in economic, social, and cultural aspects, advocating for sustainability, enriching education and practical learning, boosting careers and businesses, encouraging impactful and innovative actions, aiding sustainable expansion and diversification, engaging in the global community, forging partnerships, and endorsing self-empowerment.

Core Standards of Professional Conduct:

The ECC maintains the utmost professional integrity following the Nolan Principles, which include selflessness, honesty, integrity, objectivity, accountability, transparency, and leadership.

Application:

The core principles, values, and guidelines are meant to be consistently maintained in every aspect of the University's functioning. They represent the ethical benchmarks endorsed by the Executive Board and Board of Management, obligating all ECC members to adhere to them. Both ECC and its overseeing body are committed to fostering and preserving ethical conduct among employees, students, and stakeholders. The Ethical Framework serves as a compass for ECC members, steering their behaviors and choices, while regular assessments confirm the continual upholding of the most stringent ethical standards.

From Policy to Practice:

In every engagement, ECC, along with its members and associates, pledges to uphold equality, rejecting all forms of discrimination. They embrace diversity, prioritize safety, safeguard personal data, refrain from endorsing specific beliefs, champion environmentally conscious practices, endorse academic pursuits, honor intellectual property rights, and prioritize fundamental human rights in all dealings with individuals, businesses, and entities. ECC handles complaints with professionalism, honors obligations, pursues ethically sound funding, conducts research with ethical standards, and ensures transparent, equitable employment terms and a secure workspace for its entire staff.

Students:

ECC views students as collaborators in the educational setting, esteeming and honoring them. The institution offers comprehensive, high-quality instruction and learning chances, equitable and clear evaluations, appropriate educational resources, assistance for students with disabilities, and unbiased academic and personal guidance for all students.

Stakeholders:

ECC holds its stakeholders in high regard, aiming to fulfill their needs through providing precise public information, upholding exceptional service levels, and delivering top-notch reports, training, and services.

Local Communities:

ECC demonstrates care and regard for the communities it operates in, aiming to address their needs, navigate potential conflicts sensitively, engage in local initiatives, and enhance the surrounding environment. The company advocates for ethical conduct within its workplace and encourages similar standards from its members and collaborators.

ECC Academic Partnerships Ethics Statement:

The ethical guidelines at ECC are based on core principles that emphasize honoring people's humanity, dignity, and ways of life, supporting free expression, fostering personal growth, and promoting responsible environmental and social behaviors. ECC is dedicated to creating an inclusive environment and conducting ethical dealings with everyone involved. Partners collaborating with ECC are urged to align with these goals and be mindful of regional and cultural variations while collaborating.

IT Policy

Introduction:

The European City Campus (ECC) highly values information, using it across various domains such as learning, research, administration, and management. They've established a policy focusing on governing, securing, and responsibly utilizing ECC's information by all involved parties. It's crucial for all ECC IT system users to acquaint themselves with this policy.

The primary guidance for ECC's information security and assurance framework lies within the Data Protection Policy. This document outlines top-notch practices in information security and should be studied alongside other pertinent guidelines.

Regular reviews and updates are planned for this Information Security Policy and its related policies. These revisions will be prompted by significant developments impacting ECC's overall security stance. Users will be promptly notified of these alterations via the Intranet and direct communications. Additionally, necessary assistance will be provided to implement any new features or behavioral adjustments.

Purpose:

The main aims of this policy are:

1. Offering direction to ECC's staff, students, and users regarding the protection of ECC's information and software.

2. Safeguarding ECC's IT resources and services from unauthorized access, breaches, disruptions, and other risks.

3. Guaranteeing ECC's information remains confidential, integral, and accessible.

4. Ensuring adherence to applicable laws and regulations, allowing ECC to meet security benchmarks like Cyber Essentials and Payment Card Industry Data Security Standards Compliance (PCI-DSS).

5. Preventing the loss, exposure, or alteration of personal data and intellectual assets owned by ECC, its staff, and students.

Scope:

This guideline pertains to all individuals utilizing ECC's IT resources, encompassing hardware, software, data, network access, third-party services, and online platforms offered or coordinated by ECC. It includes any information produced, received, or stored as a result of ECC's operations. Safeguarding and managing this data should align with its level of sensitivity, importance, and worth, irrespective of where or how it is stored or accessed. ECC's Data Classification Policy offers direction regarding the identification and administration of sensitive information.

Policy Statement:

The ECC Information Security Policy's goal is to safeguard ECC personnel, students, and users from information security incidents that could disrupt their authorized activities. It prioritizes educating ECC's users on security risks and recommended actions, empowering them to effectively manage security matters in their everyday routines.

Responsibilities:

The primary duty for maintaining information security at ECC lies with the System Administrator. They're accountable for safeguarding ECC's information and its systems and ensuring that employees, students, and authorized individuals comply with all applicable policies.

Users of ECC IT equipment and services are individually accountable for following these policies and promptly reporting any breaches, security risks, or identified weaknesses.

For better clarity and application of this policy, it's categorized into three primary responsibilities: ECC IT System users, encompassing both users and providers of ECC IT Systems, and ECC IT System providers.

User Responsibilities:

Handling Sensitive Information:

Individuals utilizing ECC's IT services come across various data, some of which might not have clear classifications. When faced with such instances, users should treat the information as sensitive. This involves appropriate handling, especially if it includes personal details, sensitive personal information, potentially crucial commercial data, data related to cardholders or banks, user account credentials, or configuration specifics for ECC's information systems.

Conduct:

Those using ECC IT services are required to behave reasonably, following the guidelines soon to be outlined in the Acceptable Use Policy. This involves refraining from causing offense or distress, complying with laws, and avoiding any involvement with illegal, offensive, defamatory, or extremist content when creating, downloading, viewing, storing, or sharing materials.

Disciplinary Action:

Breaking ECC rules can result in various consequences, spanning from warnings to job loss or being expelled from a course. Claims of not following the rules due to not knowing them, having good intentions, or making a mistake won't be considered as valid reasons.

Access to Sensitive Data:

ECC utilizes access control systems to safeguard sensitive information, employing a combination of physical and logical controls. Users must adhere to the instructions outlined in this policy as well as other associated documents like the Acceptable Use Policy and Payment Card Data Protection Policy.

Data Loss Prevention:

ECC employs strategies for Data Loss Prevention (DLP) to minimize the chances of accidental or deliberate data exposure, compromise, or loss. These strategies specifically target ECC's highly sensitive data, encompassing personal and sensitive personal information. Users will receive alerts if their actions are identified as potential DLP breaches.

Physical Security:

ECC is currently creating a Physical Access Control Policy that outlines regulations and obligations for staff, students, and guests regarding access limitations. Adherence to these rules is compulsory and involves wearing ECC identification cards, refraining from unauthorized entry alongside others, and following the Clear Desk policy to prevent unauthorized access to physical materials and documents.

Protection of Data in Transit:

Confidential information should be sent using strong encryption techniques. Detailed instructions regarding the treatment of payment card data will be detailed in the forthcoming Payment Card Data Protection Policy. Additionally, the Data Classification Policy, which is currently being developed, offers additional guidance on managing data with varying levels of sensitivity.

Disposal of Stored Data:

Information that's no longer required should be securely eliminated, irrespective of its format or where it's stored. When online data is designated for deletion, it should be promptly removed or kept as per defined retention durations. Data stored on digital mediums should be securely erased using authorized techniques, while physical copies must be safely destroyed, typically through shredding.

Security Awareness and Procedures:

All individuals using ECC must acquaint themselves with this policy and its associated guidelines. Supplementary resources are accessible on the IT Services internal website to enhance understanding of the policy, procedures, and guidelines. It's mandatory for employees to finish essential IT security training programs and undergo annual refresher training.

System and Password Policy:

The ECC sets clear standards for password strength, such as minimum length and diverse character types, while also disallowing easily predictable passwords. It's crucial to keep passwords confidential, refrain from writing them down, and avoid sharing them. Additionally, the ECC mandates Multi-Factor Authentication (MFA) and expects users to follow specific guidelines for managing passwords.

Anti-Virus Policy:

ECC enforces malware defense across all ECC devices, using rigid settings that users cannot modify. The antivirus software receives regular updates to ensure current protection. Adhering to PCI-DSS standards, it is mandatory to maintain logs for antivirus product compliance.

BYOD (Bring Your Own Device):

Users must ensure that their non-ECC devices are equipped with sufficient antivirus software when used for work purposes. Certain tasks and projects might impose limitations on the utilization of non-ECC devices.

Patch Management Policy:

ECC necessitates consistent software updates and patches to tackle vulnerabilities. Users must comply with patch management standards, allowing exceptions solely upon specific approvals.

Use of Privileged Account:

Exercise caution when using accounts with high privileges, limiting their usage solely to their designated functions. Avoid employing these accounts for activities like browsing the internet or accessing emails, except when necessary for specific tasks related to MS Azure access.

Administration Access to a Device:

ECC grants users specific administrative permissions on designated devices, contingent upon following a defined procedure to acquire this access. The duration for which administrative privileges are available is restricted.

Secure Application Development:

The ECC approves software utilized for business use and mandates that all business-related items must come from authorized vendors, ensuring their recognition and approval. Additionally, these products must adhere to specifications that include integrated information security measures.

User and European City Campus's Joint Responsibilities:

Remote Access Policy:

All off-site access is safeguarded through Multi-Factor Authentication (MFA). Once remote access is no longer needed, it should be promptly terminated. To ensure secure access, various measures such as Vulnerability Scanning and Management Policy, Configuration Standards, Change Control Process, Audit and Log Review, Monitoring, Penetration Testing, and policies for Joiners, Leavers, and Movers are implemented.

Wireless Policy:

ECC ensures security by maintaining distinct wireless networks for its employees and students, aiming to protect ECC's data. Adherence to PCI-DSS standards means that payment card transactions should not be conducted through ECC's internal Wi-Fi service.

Reporting:

Any instances of confirmed or suspected policy breaches need to be promptly reported to IT Services. Devices that breach the policy can be brought to IT Services for resolution.

Failure to Comply:

Failure to follow this policy could lead to losing access to ECC ICT Systems and facing disciplinary measures. We value your cooperation in following ECC's IT policy and procedures, ensuring the safety of ECC's information, network, services, and those of our partners and third-party providers. If you require help or have inquiries, reach out to the IT Service Desk or the IT Security team at IT@europeancitycampus.lk. Your compliance is greatly appreciated.

Prevent Policy

1. Introduction

The Office for Students (OfS) supervises higher education institutions' efforts to prevent individuals from becoming involved in terrorism. To support this directive, the government has issued a set of legal guidelines. To meet its Prevent duty, the European City Campus (ECC) must:

- Create effective support systems for student welfare, enabling communication with DFE Prevent coordinators, local authorities, or the police when needed.
- Establish procedures for evaluating and reducing risks linked to external speakers and events on campus, while maintaining the commitment to uphold freedom of expression.
- Arrange continuous Prevent training for relevant staff members.
- Enforce an IT usage policy and, when applicable, a research policy.

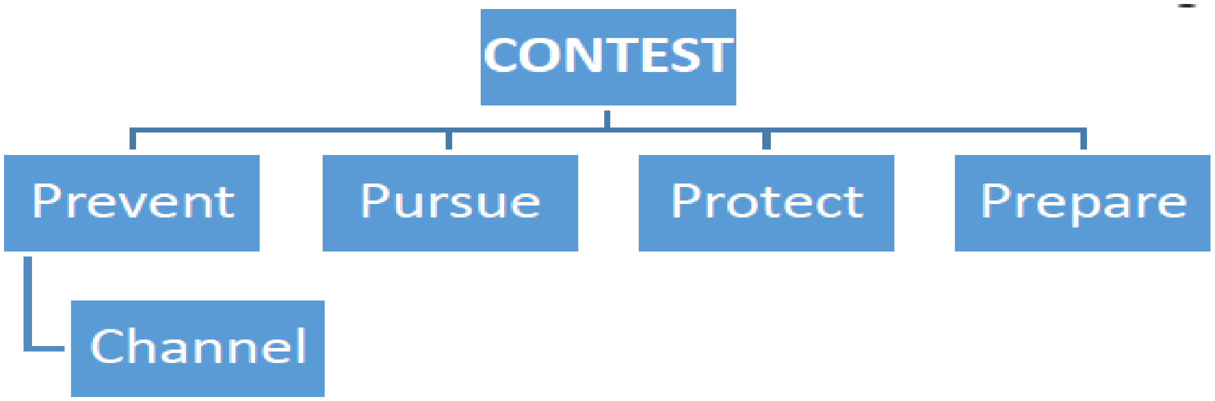
2. Scope

This policy outlines ECC's obligations in adhering to the Prevent responsibilities outlined in the Prevention of Terrorism Act (specifically No. 48 of 1979, 10 of 1982, and 22 of 1988). In compliance with legal requirements and the Revised Prevent duty guidance, ECC conducts an annual Prevent Risk Assessment and adjusts its Prevent Action Plan when needed. The policy is divided into three sections:

A. Legal Framework
B. Enforcing the Prevent Duty on Campus
C. Reporting Concerns Related to the Prevent Duty on Campus

A. Legal Framework

The Prevent strategy, part of the national counter-terrorism plan called CONTEST, aims to diminish the terrorism risk in Sri Lanka by stopping individuals from becoming terrorists or backing terrorism.



B. Enforcing the Prevent Duty on Campus

1. Prevention Action Plan
 - The Prevent Action Plan, accessible to the public, outlines ECC's yearly activities to fulfill its Prevent commitment. It undergoes annual review and modification. Contact the ECC Chair of the Data Protection Committee at DPO@europeancitycampus.lk for a copy.

2. Information Sharing (Prevent)

External Information Sharing
 - ECC has an agreement with external partners to share information lawfully under specific acts. Only the ECC Chair of the Data Protection Committee is authorized to share personal data.

Internal Information Sharing
 - Personal data can be shared among ECC Departments/Faculties for valid reasons or safety concerns. ECC follows an Internal Information Sharing Protocol. Copies of this agreement are available upon request.

3. Information Technology and Filtering
 - ECC respects academic freedom while outlining usage policies for computer facilities, including filtering arrangements and access to sensitive material.

4. External Speakers and Events
 - ECC upholds freedom of expression within legal boundaries on and off-campus. Its policy details event organization processes, measures for constructive discourse, and guidelines for using ECC premises.

5. Freedom of Speech
 - Protocols are set for contentious meetings or activities at ECC. Disputes regarding Freedom of Expression procedures are referred to the CEO and may be appealed to a special committee.

6. Academic Freedom and Sensitive Research
 - ECC acknowledges academic freedom and the importance of sensitive research, ensuring responsible access to materials related to terrorism. Approval from the CEO is required for visiting speakers.

7. Prevent Training
   - Staff undergo Prevent Duty training to understand reporting mechanisms and ECC's obligations. Refresher courses are required every three years. Students involved in specific placements or authorities may also undergo Prevent training.

C. Reporting Concerns Related to the Prevent Duty on Campus

1. The Student Coordinator oversees Prevent-related cases, managing welfare and academic support services both within and outside the university. They also implement Channel recommendations.

2. It's important to discuss any Prevent concerns in a secure and supportive setting to properly evaluate them and take suitable action.

3. The Prevent Coordinator manages cases related to the Prevent obligation, organizing welfare and academic support services within and outside the university. They're also in charge of handling Channel recommendations.

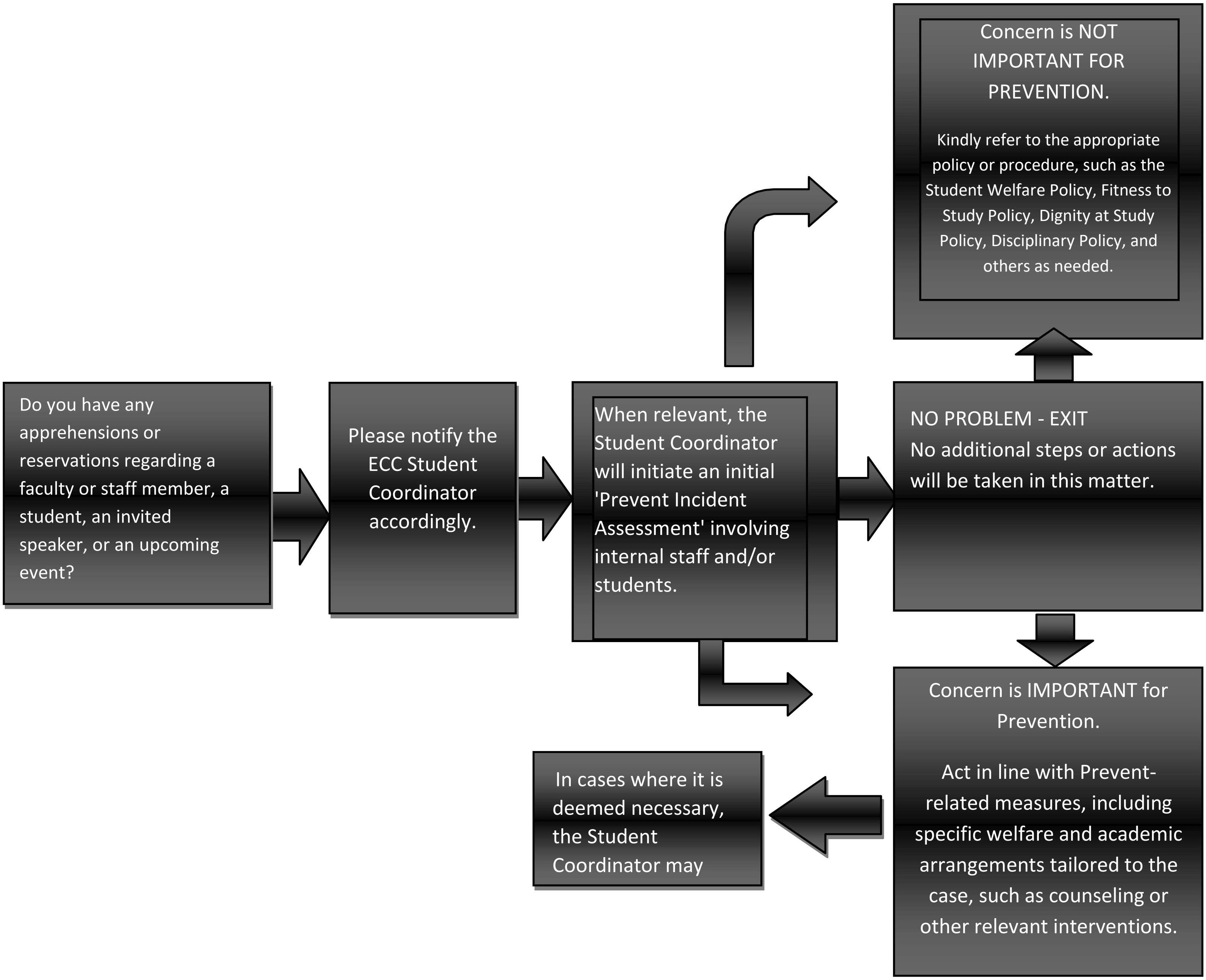
4. When a Prevent issue arises, discussing it in a safe environment is crucial. Depending on its severity and relevance:
   a) Unrelated concerns are referred to the appropriate policy/process.
   b) Less severe Prevent-related issues prompt internal welfare/academic actions like counseling, medical or chaplaincy referrals.
   c) Serious Prevent-related issues are referred to the local Channel Panel by the Student Coordinator.
   d) Cases without concerns are closed without further action.

When sharing information with third parties, ECC follows the Data Protection Act and its external Prevent Information Sharing Agreement, allowing data sharing within ECC for legitimate business purposes.

Prevent Referral Process Flowchart

For detailed guidance on the ECC Prevent Referral Process, please refer to the visual flowchart below. It outlines steps for making a Prevent referral within the ECC community, ensuring a clear and consistent process.

The ECC Prevent Referral Process



Do you have any apprehensions or reservations regarding a faculty or staff member, a student, an invited speaker, or an upcoming event?

Please notify the ECC Student Coordinator accordingly.

When relevant, the Student Coordinator will initiate an initial 'Prevent Incident Assessment' involving internal staff and/or students.

Concern is NOT IMPORTANT FOR PREVENTION.

Kindly refer to the appropriate policy or procedure, such as the Student Welfare Policy, Fitness to Study Policy, Dignity at Study Policy, Disciplinary Policy, and others as needed.

NO PROBLEM - EXIT
No additional steps or actions will be taken in this matter.

Concern is IMPORTANT for Prevention.

Act in line with Prevent-related measures, including specific welfare and academic arrangements tailored to the case, such as counseling or other relevant interventions.

In cases where it is deemed necessary, the Student Coordinator may

Staff and students should not evaluate potential risks on their own or interrogate individuals about their worries. It's crucial to promptly report any concerns that arise. If you have questions or concerns, reach out to the Data Protection Committee at DPO@europeancitycampus.lk.

Social Media Policy

1. Purpose and Scope

1.1 Introduction

The European City Campus (ECC) acknowledges the strategic significance of utilizing social media to establish effective communication and foster relationships with various stakeholders such as prospective and current students, alumni, faculty, parents, and the community. The institution recognizes the dynamic nature of social media, where personal and professional aspects occasionally intersect.

1.2 ECC Values and Behaviors

The values and behaviors upheld by ECC are integral to its institutional identity, emphasizing the need for these principles to be accurately conveyed in all interactions, including public engagement on social media platforms.

1.3 Content

This document is divided into three sections, each intended to ensure the consistency of our online presence with the aforementioned values and behaviors.

1.4 Best Practice

1.4.1 ECC acknowledges and embraces the advantages and opportunities presented by social media, benefiting both the institution and its stakeholders. Upholding best practices and empowering staff and students on social media are crucial for establishing exemplary standards within ECC.

1.4.2 This approach, at the institutional level, ensures authenticity, fosters a positive brand perception, and enhances our outreach, enabling the transmission of core messages securely and appropriately. At an individual level, leveraging the ECC reputation and becoming an integral part of the brand identity can result in empowerment and recognition.

2. Policy Statement

2.1 Within this policy's scope, social media refers to interactive online platforms that enable immediate communication between individuals or the sharing of messages in a public setting.

2.2 It acts as a tool for disseminating news, updates, and achievements, ensuring all involved parties stay informed about important developments. Furthermore, it fosters productive discussions in academia regarding contentious subjects and research areas.

2.3 Despite its benefits, using social media carries inherent risks due to its instant and widespread reach. Inappropriate use could negatively impact the university's staff, students, and overall reputation.

2.4 The Marketing Subcommittee Chair holds responsibility for overseeing this policy. Any content considered inappropriate, offensive, or illegal should be first reported to the Marketing Subcommittee Chair, who may escalate issues within the Subcommittee if necessary.

2.5 The Marketing Subcommittee Chair bears accountability for the content, and violating the policy could lead to legal or disciplinary actions against the users involved.

3. Ensure compliance with the law

3.1 Social media accounts are established and owned by ECC. If an individual's name is connected to a department or club account, ownership rights are given up unless a transfer of ownership is coordinated with the Marketing Subcommittee Chair.

3.2 Before creating any social media accounts, proposals must be sent for approval to the Marketing Subcommittee Chair. A comprehensive business case is necessary for new channel creation, including available resources for managing the account, a well-defined content strategy, and a solid business proposal.

3.3 All ECC-affiliated social media accounts must be connected to either a department's administrative email or an employee's work email. The central social media team should have access to all account passwords to ensure continued access even if an employee leaves ECC.

3.4 ECC employees are not allowed to use personal email accounts for ECC-related social media accounts. Each account must provide administrative access to multiple ECC employees, with the understanding that this access might be revoked due to an employee leaving, being reassigned, or facing disciplinary measures.