Data Protection Policy

1. Policy Statement

1.1. It is the policy of St. Constantine's International School to secure all "restricted" and "sensitive" data. This includes the data that is stored electronically. The details of this policy list how different data is to be handled to comply with this policy.

2. Reason for Policy

2.1. Data used by the School often contains detailed information about the School, as well as personal information about School students, faculty, staff, and other third parties affiliated with the School. Protecting such information is driven by a variety of considerations including legal, academic, financial, and other business requirements.

2.2. Regardless of where the data resides, the School has legal and ethical obligations to ensure that this data is managed in a manner that maximizes its utility while minimizing risk of unauthorized or inappropriate use or disclosure.

3. Who Should Know This Policy

3.1. All areas of the school are governed by this policy (support staff, admin, teachers, students)

3.2. Third party and consultants must follow this policy.

4. Definitions

4.1. *Public* - Information that may or must be open to the general public that has no existing local, national, or international legal restrictions on access.

4.2. *Restricted* - Information protected due to protective statutes, policies, or regulations. This level also represents information that isn't by default protected by legal statute, but for which the Information Owner has exercised his or her right to restrict access.

4.3. *Sensitive* - Information protected due to proprietary, ethical, or privacy considerations. This classification applies even though there may not be a direct statutory, regulatory, or common-law basis for requiring this protection.

4.4. *Critical Data* – Data that is needed to conduct school business.

5. Policy Details

5.1. Users are to use only those technology resources that they are authorized to use and use them only in the manner and to the extent authorized.

5.2. Users are to protect the confidentiality, integrity, and availability of technology resources.

5.3. Users are to comply with all applicable school policies.

5.4. Users are responsible for any activity performed using their usernames and passwords except when account security is compromised by actions beyond the user's control.

5.5. Users are responsible for ensuring that critical data are backed up and available to be restored for systems not administered by Information Systems Technology. This includes critical information contained on technology devices oriented to individual use (e.g., desktops, laptops, smart phones, and similar such devices).

5.6. Users are responsible for ensuring that "sensitive" and "restrictive" data to which they have access is guarded against theft, and inappropriate disclosure.

5.7. Removable Storage (e.g. USB Sticks, Flash Drives, External Hard Disks)

5.7.1. "Sensitive" classified data should not be stored on removable storage.

5.7.2. "Restricted" classified data on removable storage must be encrypted with a strong password

5.7.3. Removable storage must be disposed of properly (this means wiping it clean before disposing)

5.8. Screen Saver Password must be implemented

5.9. Data Stored in the Cloud

5.9.1. "Sensitive" classified data should not be stored in the cloud.

5.9.2. "Restricted" classified data must be encrypted with a strong password

6. Violations

6.1. Contact the IT Technical Support team with your concerns.

Policy Reviewed **23/05/2019**

Next Review Date **19/05/2020**