The Student Robotics Club Of South Australia Incorporated
Data Protection and Information Security Policy

June, 2015

Classification: Public

Table of Contents

1 Change Register

Version	Date	Description	Author
1	20/06/15	Initial Draft	DA

2 Introduction

The protection of the personal information and privacy of our members is very important. The majority of sensitive information which the club manages is in relation to information on our members. This document outlines the processes, controls and policies in place to manage risk to our information assets including member's personal information.

3 Scope

This policy applies to all information collected and managed by any member of the club on behalf of the club. Information shared by members for personal purposes is not part of the clubs information assets and thus not considered here.

An Information Asset Register will be maintained and is referenced in Appendix A. This register will identify all assets covered by this policy.

4 Risk Assessment

Threats to the information assets identified in Appendix A will be reviewed at least annually my the management committee. Where relevant the corresponding risks will be included in the club's Risk Register.
It has been identified that the ongoing and generic risk we face from an information security perspective are:

- Accidental exposure of personal information through incorrect handling or weakness in access controls
- Malicious attacks through email messages directed to members
- Misuse of information by service or hosting providers

5 Information Classification and Handling

To appropriately protect information in the custody of the club, the following classification system and related handling guidelines has been developed. Each asses in the Information Asset Register will be entered with a related classification. Suitable controls (as specified below) will be established to suitably protect information assets according to their classification.

Classification	Description/ Examples	Handling
Public	Information either required to be published, marketing material or information that would have no impact if it were publicly released. Examples include advertising and club description, constitution and policies to be published on the website.	No special handling is required.
Club Use	Information available to all club members but not suitable for public distribution. This information may cause minor	Storage in the club's Google Drive and accessible to Domain Accounts. This information can be sent via email and forwarded to personal accounts as

	impact to club operations or competitive advantage.	long as the classification of the information is made known to the receiver.
Administrative	Information which is useful to the running of the club but necessary or appropriate for student members to access. This may include insurance, financial and disciplinary or performance assessment information.	Storage in the club's Google Drive and accessible to Members of the Management team. This information can be sent via email and forwarded to personal accounts as long as the classification of the information is made known to the receiver. No restriction is placed on communicating with adult members. Information can be disclosed to student members are due consideration.
Confidential	Information which is of high personal value or required to be protected by law. Exposure of this information would cause a significant impact to an individual. Personally identifiable information, Health Information or information which is required to be protected by regulation. Information related to complaints or misconduct.	Storage in the restricted directories of the Google Drive. Access will be granted to specifically designated officers of the club based on their assigned roles. This information is not to be sent via email outside of the Google domain. Any communication outside of the designated officers should only be performed in compliance with legal obligation or after consulting the management committee. Any printed copies or copies on removable media must be securely destroyed.

All documents are to be marked with their classification.

6 Policy Controls

6.1 Domain Accounts

Each member will be given a unique Domain Account for accessing shared resources and receiving club communication. Unless the member is handling Confidential information, this email address can be forwarded to a personal email address outside Gmail.

Where a member has administrative access to impact or alter security controls, they will be provided an additional Domain Account which has the elevated access privileges to perform these actions. This account will not be used to communicate by email. Access to this account will require two factor authentication. This provides protection by limiting the impact of phishing attacks on the member's email access.

Each member is accountable for all access and activities performed by their allocated domain account(s). Misuse of their account(s) may result in disciplinary actions.

A policy will be implemented to enforce strong passwords for all domain accounts. This will reduce the risk of exposure through password guessing or brute force attacks.

An annual review will be performed to ensure that administrative access is still appropriate. When a member is found to no longer be engaged in a role, they will be removed from privileged access.

When a member does not renew their membership, their domain account will be locked and no access will be allowed.

6.2 Data Storage

Google has been selected as a trusted service provider. Due to their size and proven integrity, their systems have been identified as suitably secure for our operations.

Organisational data will be stored on the Google drive and access restricted to domain accounts only.

Specific folders will be established to protect Administrative and Confidential information. A routine review will be conducted to ensure that the permissions on the Administrative and Confidential folders is correct.

Information provided on paper will be scanned and stored on the Google Drive. The paper will then be shredded.

Information can be temporarily stored on private systems for editing and maintenance but must be suitably transferred and removed when complete.

6.3 Servers and Applications

A server is maintained by the system administrators to run the website. This server will be maintained and secured against common security vulnerabilities.

Web applications which are developed to transfer Administrative or Confidential information will ensure that all requests are encrypted and use a publicly verifiable certificate. This will minimise the risk of exposure of information in transit.

No member's financial account information will be accepted by the club. If a payments page is enabled, the web application will redirect all payment transactions to the Bank or Google's payment services. All other payments will be conducted via cash, cheque or payment transfer initiated by the member.

All information captured by the web application will be transferred to the Google Drive for secure storage.

7 Appendix A Information Asset Register

Asset	Description	Classification
Club Incorporation documents	These are the documents describing our club.	Public
Policies	These documents describe how we meet our obligations and minimise risk to our members.	Public
Club meeting minutes	Minutes from Management and General meetings	Public or Club Use depending on content
Media information	Press releases, advertising material, presentations, etc.	Club Use or Public depending on release status.
Attendance Records	Information on active members and their involvement.	Club Use
Photos and Videos of events	These files may depict students or club members in activities of the club.	Club Use unless specific release permission has been granted.
Competition Information	This maybe project plans, designs, strategies, BOM or running notes relating to the conduct of the current competition.	Club Use
Financial Records	Club Bank account information Bank statements	Administrative
Sponsorship and Grant Information	Conditions of grant terms, amount and tracking details for expenses.	Administrative
Completed Membership forms	These forms contain personally identifiable information and health information.	Confidential