CSSC Information Security Policy

Purpose

The CSSC Information Security Policy (ISP) is concerned with protecting the system, equipment and processes of CSSC that support keeping information safe and protected, no matter how, or in what form, the information is either held, processed or shared.

Policy

CSSC is located at Compton Court 20-24 Temple End, High Wycombe, Bucks, HP13 5DR and operates primarily in the business of the management and provision of sport and leisure opportunities to its members (from the Civil Service and Public sector) and in the support and training of its volunteers.

Through the implementation of the ISP which incorporates CSSC's Information Security Management System (ISMS) and relevant policies including the Information Technology Security Policy (ITSP), CSSC makes sure that all persons having access to members' information can be held accountable for their actions and is committed to protecting and preserving the information's:

- Confidentiality: by not allowing information to be seen by anybody who does not have the right;
- Integrity: by making sure that the information is always accurate and complete;
- Availability: by making sure that the information is available only to authorised users when required to conduct our business.

Since their design, development and agreement, the CSSC ISP and ITSP have:

- Been socialised, reviewed and supported in full by the ET
- Been disseminated to all Managers and onwards to their staff
- Been read and the implications of it understood by all staff who have been required to sign declarations to this effect
- Been reviewed to ensure it continues to be aligned with the organisations goals
- Been summarised into a desk aid provided to frontline staff, detailing the critical information needed to support their daily adherence to this policy.

The ISMS is intended as a mechanism for managing information security related risks and improving the organisation to help deliver its overall purpose and goals. The online platform environment and the approach taken to risk assessment and management, the Statement of Applicability and the wider requirements set out for meeting ISO 27001:2013 identify how information security and related risks are addressed and information protected.

For our ISMS:
- The information security policy and objectives are established and in line with the strategic direction of the organisation
- Integration of the ISMS has been made into the organisations processes
- Resources needed for the ISMS are available

- Communication covering the importance of effective information security management and conformance to the ISMS requirements is in place
- The ISMS achieves its intended outcome(s)
- Contribution of persons involved in the effectiveness of the ISMS has been made by direction and support
- Continual improvement is promoted
- Legal and contractual requirements are complied with
- Other management roles within their area of responsibility are supported
- The ISMS manual has been reviewed and updated to align it with ISO/IEC 27001:2013

Information and information security requirements will continue to be aligned with the organisation's business goals and will take into account the internal and external issues affecting the organisation and the requirements of interested parties. An internal audit / review of procedures and policies is conducted annually. In addition, achievement of the quality objectives are measured against quarterly targets set in relation to the business plan.

All employees and relevant interested parties associated to the ISMS have to comply with this policy.

We are committed to achieving and maintaining certification of the ISMS to ISO27001:2013 along with other relevant accreditations against which our organisation has sought certification.

The CEO is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the requirements set out in ISO 27001:2013.

A current version of this document is available to all members of staff and is displayed on our website.

This policy will be reviewed regularly to respond to any changes in the business, its risk assessment or risk treatment plan, and at least annually.

Andy Shaw, Director of Volunteering and Business Delivery

3/9/19

Document Control

Version	Date	Summary of changes	Changes marked	Approved
0.1	15.8.17	Initial version		AS
0.2	06.8.18	Review to reflect actions from GDPR		AS
0.3	27.9.18	Review to reflect actions following use of ISMS online		AS
2.0	10.07.19	Reviewed and updated.		AS