IT & Information Security Policy

1. Policy Statement

Farnham Angling Society (FAS) adheres to the General Data Protection Regulation (GDPR), with respect to all information held about Members and Officers. The Society is a Data Controller and is registered with the Information Commissioner's Office - Registration Number A8395852.

The Data Protection Officer is Ian Gray and can be contacted via email at GDPR-DPO@farnhamanglingsociety.com

This Information Security policy:

- Defines the IT and Information Security Policy for Farnham Angling Society.
- Sets out the FAS high-level requirements for the management of Information Security in relation to the storage, processing and transmission of confidential data.
- Meets the compliance obligations to the Payment Card Industry Data Security Standard (the PCI DSS). Version 3.0, released in November 2013, in particular the standards for merchants with payment application systems connected to the Internet, no electronic cardholder data storage (SAQ C)

The PCI Data Security Standard specifies 12 requirements for compliance, organized into six logically related groups called "control objectives".

Control Objectives	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system password and other security
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software on all systems commonly affected by 6. Develop and maintain secure systems and
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

2. IT & Information Security Policy

2.1 Purpose

This document details the IT security strategy for FAS in relation to the storage, processing and transmission of confidential data including credit card data. Its aim is to set out the Information Security responsibilities for staff, contractors, partners and third parties.

This document should be reviewed:

- At least annually when the FAS undertakes its annual PCI compliance review.
- If any new credit card processing or IT systems or processes are implemented.

2.2 Roles and Responsibilities

The Executive Committee will identify a lead person, with responsibility for ensuring that the aims set out in this policy document are observed and monitored, together with the reviewing this policy. The FAS IT Security lead may be:

- One of the Executive Committee Members, who will be provided with appropriate training if required
- A designated manager, again, with training if required
- An IT Security specialist appointed by the Board

The FAS IT Security lead is responsible for:

- Overall responsibility for Information Security and related issues.
- Development and maintenance of Information Security Policies and Procedures
- Communication and review of Information Security Policies.
- Coordination of PCI Security Audit Tasks.
- Coordination with PCI Accredited Security Auditors (Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs))
- Keeping the Board updated on all security related issues.

The Farnham Angling Society management team are responsible for ensuring that the requirements of this policy are adhered to, including responsibility for:

- Ensuring that staff are aware of the IT Security policies and procedures.
- Ensuring that the requirements of the IT Security policies and procedures within their control are adhered to.
- Reporting IT Security incidents or concerns to the IT Security lead and participating in implementing actions where required.

3. IT Security Audits

Regular audits of IT Security will be undertaken, in line with the requirements of the PCI standards, and other standards, as appropriate.

3.1 Annual Policy Review

All Information Security Policies are reviewed and where necessary updated on at least an annual basis. The review process ensures that:

- Policies in place are still required.
- Perceived threats facing FAS are identified and consideration included in procedural documentation.
- Any new legal issues are identified that require changes in current policy or practice.
- FAS meets current PCI compliance standards.
- Any changes to network configuration or new applications are included in the security policy.

A formal documented risk assessment process should also be completed annually to identify key business assets (including credit card data stores and supporting networks), and potential threats and vulnerabilities, which could impact on the security of those assets.

3.2 Breaches of this policy

FAS is committed to ensuring that our IT Security policy is effectively implemented. Any breaches of this policy coming to the attention of management and/or directors will be dealt with appropriately.

3.3 Security Training

All staff will receive security awareness training as part of their induction and at least annually.

FAS shall also ensure that vendors, contractors, and business partners covered by this policy are familiar with its requirements.

Staff with cardholder data access:
Staff with privileged access, deemed to have the need to know (see PCI DSS Requirement 7) should be given extra training.