St Albans Rugby Club, Oaklands Lane, St Albans
Hertfordshire, AL4 OHR
Tel: 01727 869945

St Albans Rugby Football Club

Data Security and PCI DSS Policy

St Albans Rugby Football Club

Data Security and PCI DSS Policy

Background

There are multiple laws and schemes which cover the use of personal data by the club.

- Customer and club member data is protected by the Data Protection Act.
- General use of computers is covered by the Computer Misuse Act.
- Handling of payment card data is covered by the Payment Card Industry Data Security Standard.

The club must ensure it has appropriate measures to secure the data we use.

Data Protection Act

Customer and club member ('personal') data must be treated in accordance with the principles of the Data Protection Act.

- The club must keep a list of all databases containing personal data (other than the RFU Game Management System which is used as standard)
- Use of any such database must be approved by the Club Chairman.
- Everyone stored in the database must have consented to their data being stored.
- Consent should be clearly identified as part of the membership process.

PCI DSS

PCI DSS is a scheme run by the payment card industry to ensure that card holder data is not misused.

The club is subject to PCI DSS because we take card payments at the bar via WorldPay.

Card data refers to the long card number (PAN), the short number on the signature strip (CVV2) and the card expiry date.

- No card data should be written down and stored by staff or club members.
- All card receipts should be stored in the till.
- These receipts must all be sent to the Honorary Treasurer as quickly as possible for storage.
- Only committee members should handle these receipts once placed into the till.

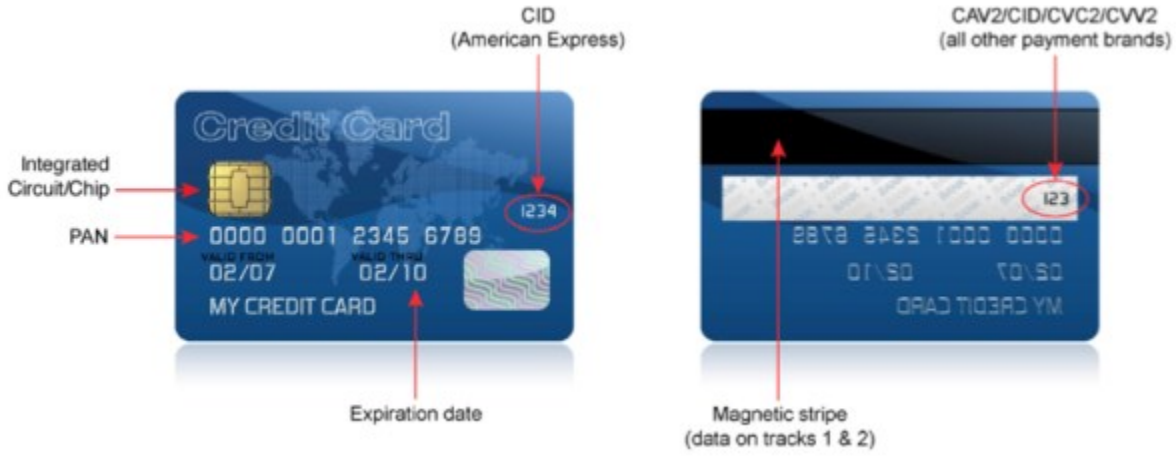
Computer Misuse Act

This act covers access to computer systems to which an individual is not authorized.

- The club and all members with access to relevant computer systems must comply with any restrictions on the use of those systems
- User names and passwords must be unique to the individual they are provided to (not shared), they should be protected from being discovered (not written down) and must not be disclosed to another person.

St Albans Rugby Football Club

How we handle card payments



It is our responsibility to ensure card holder data is never stored and is processed properly

Only use the card payment machine according to instructions

Ensure you have had training before using the machine

Do not write down any card data

Store all receipts from the card machine in the till

Data Protection Act principles

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

- at least one of the conditions in Schedule 2 is met, and
- in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Personal data shall be accurate and, where necessary, kept up to date.

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

About the rights of individuals e.g.[11] personal data shall be processed in accordance with the rights of data subjects (individuals).

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Personal data should only be processed fairly and lawfully. In order for data to be classed as 'fairly processed', at least one of these six conditions must be applicable to that data (Schedule 2).

Conditions relevant to the first principle

Personal data should only be processed fairly and lawfully. In order for data to be classed as 'fairly processed', at least one of these six conditions must be applicable to that data (Schedule 2).

- The data subject (the person whose data is stored) has consented ("given their permission") to the processing;
- Processing is necessary for the performance of, or commencing, a contract;
- Processing is required under a legal obligation (other than one stated in the contract);
- Processing is necessary to protect the vital interests of the data subject;
- Processing is necessary to carry out any public functions;
- Processing is necessary in order to pursue the legitimate interests of the "data controller" or "third parties" (unless it could unjustifiably prejudice the interests of the data subject).[12]

PCI DSS Requirements

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 passwords and other security parameters
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 malware
	6. Develop and maintain secure systems and applications
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 computer access
	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 processes
Maintain an information security policy	12. Maintain a policy that addresses information security

Computer Misuse Act

This act introduced the following three offences:

- unauthorised access to computer material, punishable by 12 months' imprisonment (or 6 months in Scotland) and/or a fine "not exceeding level 5 on the standard scale" (since 2015, unlimited);[7]
- unauthorised access with intent to commit or facilitate commission of further offences, punishable by 12 months/maximum fine (or 6 months in Scotland) on summary conviction and/or 5 years/fine on indictment;[8]
- unauthorised modification of computer material, punishable by 12 months/maximum fine (or 6 months in Scotland) on summary conviction and/or 10 years/fine on indictment;[9]

28th February 2017