Sydenham Lawn Tennis & Croquet Club Ltd
Security of Data Policy

This policy covers how data relating to Sydenham Lawn Tennis and Croquet Club Ltd (the 'Club') should be kept secure, be safely transferred, and safely disposed of.

There are two main audiences:

- Club employees and contractors - primarily the Club Manager, Welfare Officer (if not the Club Manager), and Head Coach, but also any other employees and/or contractors that work at the Club and have access to data. They undertake most of their work at the Club premises, but may also take data off site. They may have access to the Club computing equipment, and any other devices used for Club business, as well as Club documents.
- Club volunteers - this includes the Club Chair, Club Secretary and other Directors, and may include a Welfare Officer or reserve Welfare Officer. The majority of work will be undertaken outside of the Club premises using personal devices, such as computing equipment, mobile phones, etc. They may have access to the Club computing equipment, and any other devices used for Club business, as well as Club documents.

There are two main classifications of data:

- 'Sensitive Data'. This includes Club bank statements, contracts, HR records and membership personal data - addresses, emails, telephone numbers, bank account details, etc. Sensitive matters such as suspension, exclusion or termination of a member and reports on safeguarding issues are also Sensitive Data.
- 'Non-sensitive Data'. This includes anything excluding Sensitive Data. Board and committee minutes can be considered non-sensitive, excluding any parts of the minutes dealing with Sensitive Data.

Club Manager, other employees and contractors, and volunteers

In Club premises:

- Access to Sensitive Data should be limited to the Club Manager and other employees and contractors, and volunteers, including the Welfare Officer and reserve Welfare Officers (whether employees or volunteers) who need to have access to such data in order to carry out their role.
- No volunteer (apart from a Welfare Officer) should have access to Sensitive Data on a day-to-day basis, but some Sensitive Data may be shared with some or all Club Directors when required.
- The Club Manager, other employees and contractors, and any volunteers having access to Sensitive Data, have a duty of confidentiality regarding Sensitive Data.
- All printed Sensitive Data should also be secured at the end of each day in the bar storage area.

- Under no circumstances should Sensitive Data be left in common areas of the Club premises, where it is accessible to unauthorised personnel.
- The Club Manager and other employees and contractors should use the Club's computing equipment for the storage of Sensitive Data at all times.
- All Club computing equipment and mobile devices should be passcode protected and logged out when unattended or not in use. This equipment should be secured at the end of each day in the bar storage area.
- The bar storage area should be protected by a locked door and alarm system with a key that is restricted to authorised keyholders.

Out of Club premises:

- All employees, contractors and volunteers must exercise caution when taking Sensitive Data away from the Club premises. Only the minimum amount of data required to fulfil a business need should be taken away and secured appropriately.
- Volunteers may use personal computing equipment and mobile devices outside the Club premises. These devices should be passcode locked when not in use.
- Particular care must be taken when printing Sensitive Data outside the Club premises, and copies should not be left unattended on home printers.
- Particular care must be taken when disposing of Club documents outside the Club premises. Documents which contain Sensitive Data must be shredded before being placed in waste bins. Non-sensitive data should be torn up but need not be completely shredded before being placed in waste bins.

Club communications

Emails relating to Club business should only be sent to the relevant Club employees, contractors and volunteers. The distribution of Sensitive Data is limited as set out above.. The distribution of Sensitive Data is limited as set out above~~.~~

The Club Manager and other employees and contractors should use a @sltcc.co.uk email address for all Club communications.

Volunteers who regularly send emails for Club business, including to members and external organisations, should use a @sltcc.co.uk email address. If they do not have their own sltcc address, emails should be sent from the generic email address info@sltcc.co.uk which can be arranged through the Club Manager. ~~If they do not~~

-

- All employees, contractors and volunteers must use a @sltcc.co.uk email address to send emails/documents which contain Sensitive Data. If they do not~~If they do not~~ have their own sltcc address, emails should be sent from

the generic email address info@sltcc.co.uk, which can be arranged through the Club Manager. If they do not have their own sltcc address, emails should be sent from the generic email address info@sltcc.co.uk. If the data is confidential then the email should be encrypted and passcode protected.

Dropbox

Club employees, contractors and volunteers should file attachments in the appropriate Club Dropbox account folder. Dropbox is to be made available to the Club Manager, Club Chair, Club Secretary and other Club Directors as appropriate, and any other volunteer approved by the Board.

Access to each Club Dropbox account folder will be provided by the relevant Owner of each folder, who will also delete access when required, e.g. retiring directors. The Club Secretary will control the main SLTCC shared files folder.

The Club Manager may set up a separate Dropbox file for specific projects which will be made available to the relevant Club employees, contractors and volunteers, e.g. risk assessments and safeguarding.

If any Sensitive Data is stored on Dropbox, access to this information will be limited to such of the Club's employees, contractors or volunteers to whom it is essential that they have access to this information to carry out their role.

This policy is reviewed every three years (or earlier if there is a change in national legislation).

Chair: Gillian Bartlett

Welfare Officer: Dez Lewington

All employees, contractors and volunteers must use a @sltcc.co.uk email address to send emails/documents which contain Sensitive Data . If they do not have their own sltcc address, emails should be sent from the generic email address info@sltcc.co.uk If the data is confidential then the email should be encrypted and passcode protected.