Queens Park Tennis Club CIC
Data Protection Policy

Key contact:
Stephen Lee, Queens Park Tennis Club CIC Data Protection Compliance Lead

Who policy is intended for:
All Queens Park Tennis Club members, Guests of members, Parents and legal guardians of child members, Committee members, Directors, Coaches, Staff, Volunteers, Clubhouse key holders, Clubhouse visitors (including private hires), Contractors, Consultants, Suppliers, Pay and Play users, and other customers

Contents:

1. Policy statement

The General Data Protection Regulation (GDPR) took effect across the EU on 25 May 2018 and was retained in UK law after the United Kingdom left the European Union, as the UK GDPR. The UK GDPR applies to "personal data", which means any information relating to an identifiable living person. Along with the Data Protection Act 2018, the UK GDPR sets out the legal and regulatory framework for the safeguarding of personal data that all organisations much comply with regardless of their size.

The UK GDPR applies to any company, charity or other organisation which "processes" any personal data. "**Processing**" includes the collection, holding, use, sharing and even deletion of personal data. Processing includes almost any activity with data.

Queens Park Tennis Club CIC (QPTC CIC) needs to collect holds and use certain types of data about individuals, mainly details of their members, customers, suppliers, coaches, staff, and volunteers. Individuals whose personal data is processed are known as a **'Data Subject'**. Examples of personal data that QPTC CIC processes includes identity data (names, dates of birth etc.) and contact data (telephone numbers, email addresses etc.).

We will ensure that personal data is collected, managed and maintained appropriately, whether on paper, electronically (including e-mails produced or received), audio-visual or recorded in any other way. Data protection is essential because it helps people feel confident that their information will be used in a way they would expect. It allows them to control how others use the personal data they share with them.

QPTC CIC is what is known as a **'Data Controller'**. Data Controllers make decisions about processing activities. QPTC CIC exercises overall control of the personal data being processed and are ultimately in charge of and responsible for the processing.

Self-employed coaches are Data Controllers under GDPR for the data they process (see section 16 - QPTC Coaches).

QPTC CIC must comply with the Data Protection Principles, a set of rules for the handling of personal data. The Data Protection Principles require that personal data is:

- processed lawfully, fairly and transparently
- adequate, relevant and no more than is necessary
- accurate and kept up to date, and
- processed securely.

GDPR is regulated in the UK by the **Information Commissioner's Office** (ICO). The ICO is an independent body responsible for making sure that organisations comply with the Data Protection Act 2018. Its role is to uphold information rights in the public interest.
QPTC CIC is registered with the ICO.

2. Purpose and scope

Under data protection legislation individuals have certain rights which must be observed by QPTC CIC. This policy applies to all members, parents and legal guardians of junior players / children, non-member players, suppliers, contractors, consultants, coaches, staff, volunteers, directors, other customers and visitors (collectively referred to as Data Subjects).

This policy seeks to ensure that we:

1. Are clear about how personal data must be controlled and processed and QPTC CIC expectations for all those who control and process personal data on its behalf
2. Comply with the data protection law and with good practice
3. Protect QPTC CIC reputation by ensuring the personal data entrusted to us is controlled and processed in accordance with data subjects' rights
4. Protect QPTC CIC from risks of personal data breaches and other breaches of data protection law.

This policy sets out our legal obligations and how we will meet the requirements of the Data Protection Act (2018), focussing on how we will implement the six Data Protection principles.

It extends to all situations where QPTC CIC is the Data Controller or a Data Processor of personal data; and applies to all personal data processed regardless of the media on which the data is stored.

3. What is personal data?

Personal data is defined as any information relating to an identified or identifiable person. An identifiable person is one who can be identified, directly or indirectly. Personal data includes name, date of birth, National Insurance number, home address, email address, student ID number, visa and immigration information, photo, fingerprints.

Special Category data is a subset of personal data that requires even more protection. Examples of Special Category data include health records and equality data.

4. Data Protection principles

The foundations of the Data Protection Act are six principles which QPTC CIC must uphold. We will ensure that people's data is:
1. Used fairly, lawfully and in a transparent way
2. Used for specified, explicit and legitimate purposes
3. Used in a way that is adequate, relevant and limited to only what is necessary in relation to the purpose for which it was collected
4. Accurate and, where necessary, kept up to date
5. Kept for no longer than is necessary
6. Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

5. Key concepts

Transparency:
QPTC CIC should provide information about how they shall use personal data as soon as its first collected from individuals or from other sources. For example, QPTC CIC needs to tell individuals about their data subject rights, their right to withdraw consent; and provide information about data retention. Privacy Notices will be provided to all QPTC members, staff, volunteers, coaches, clubhouse key holders, venue hirers, contractors and suppliers; and will be brought clearly to the attention of Pay and Play users.

Processing or using personal data:

QPTC CIC can only use an individual's personal data if we have a "lawful basis" for doing so. The legal basis can affect which rights an individual has in relation to their personal data. There are **six lawful bases** for processing personal data set out in the UK GDPR:

1. **Consent:** the individual has freely given clear consent for you to process their personal data for a specific purpose. Consent must be specific and requires a positive opt-in. Individuals must be able to withdraw consent at any time. You should keep evidence of consent given– who, when, how, and what you told people. You should get separate consent for separate things.
2. **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering a contract. You do not need to have signed or created a contract to process data under this legal basis.
3. **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations). You should document your decision to rely on his basis.
4. **Vital interests:** the processing is necessary to protect someone's life.
5. **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
6. **Legitimate interests:** the processing is within the legitimate interests of the data processor and the data subject, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. To apply legitimate interest to a processing activity you need to:
    - Identify a legitimate interest
    - Show the processing is necessary to achieve it, and
    - Balance it against the individual's interests, rights and freedoms.

The Data Use and Access Act 2025 introduced a new lawful ground for processing personal data, Recognised Legitimate Interests. This gives businesses more confidence to use data for crime prevention, safeguarding, responding to emergencies, and other specified legitimate interests.

The most relevant lawful bases for QPTC CIC are Contract, Consent and Legitimate Interests.

To request withdrawal of consent, an individual can send an email for the attention of the Data Protection Compliance Lead, to: admin@qptc.co.uk

Data storage and security:

The Data Protection Act requires us to keep personal data secure, using appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

This applies to all data whether it is stored at home or at the QPTC clubhouse, or on portable devices. It is a requirement that personal data remains secure and cannot be accessed by people you share your home with or who you may share electronic equipment with.

Our security measures must line up with the sensitivity of the personal information held. Stronger measures must be in place if the information is sensitive or poses a higher risk for the person it relates to. For example, financial information that could be used for fraudulent purposes.

All personal data stored electronically should be password protected and accessible only to those granted permission to do so. Additional security measures include a strong password policy, anti-virus software, network files, encryption, use of password-protected documents as necessary, and two-factor authentication for logging into systems which hold data, including emails.

Where personal information is stored on or accessible via electronic devices, maintain security of passcodes and passwords (e.g., email passwords, ClubSpark administrator passwords, online banking log-in info) and always log out of accounts and devices.

Any paper containing personal data should either be scanned and then stored in a secure electronic system, or it should be stored in a lockable drawer or cabinet when not in use (e.g., the visitor signing-in book). Additional security measures include locks on office doors and having a no paper policy.

All personal data when no longer required must be disposed of securely. For paper records, this means shredding. When removing or deleting data from computers and electronic devices, we need to be aware that electronic systems can have back-ups or background storage.

Accountability:

QPTC CIC should be able to demonstrate compliance with the data protection principles. Keeping records of privacy notices, data processing agreements, data sharing agreements, data audit/ mapping documents as well as copies of any documentation used to collect consents from individuals is important.

Using personal data for marketing purposes:

QPTC CIC uses the personal email addresses of members for communications and newsletters, these activities are regarded as direct marketing and require the consent of individual members. For consent to be valid it must be freely given, specific and informed and it cannot be collected in an ambiguous fashion (e.g., via a pre-ticked box).

QPTC CIC will continually review the method for obtaining consent from members and customers for direct marketing and/or fundraising and the validity of consents that have previously been obtained.

A member can withdraw consent to receiving marketing emails by sending an email for the attention of the Data Protection Compliance Lead, to: admin@qptc.co.uk

6. An individual's rights under UK GDPR

Individuals have the right under the UK GDPR to know what QPTC CIC is doing with their personal data. In addition, they have the following specific rights:

- Right to request to access and receive a copy of their personal data, and other supplementary information, commonly known as a "data subject access request" (See section 10).
- Right to request correction of their personal data. QPTC CIC may need to correct any incomplete or inaccurate information that it holds, without delay, and should up-date out-of-date personal data where necessary (e.g. where it is not simply a pure historical record).

- Right to request erasure of their personal data. An individual can ask QPTC CIC to delete or remove personal data where there is no good reason for it continuing to process it.
- Right to object to processing of their personal data in certain circumstances.
- Right to request the restriction of processing of their personal data. This is not an absolute right and only applies in certain circumstances. When processing is restricted, QPTC CIC is permitted to store data but not use it.
- Right to request the transfer of their personal data to another party.
- Right to complain to the Information Commissioner.

Individuals can exercise their rights in writing by email for the attention of the Data Protection Compliance Lead, to: admin@qptc.co.uk

7. Child members

When QPTC CIC processes personal information of children under the age of 13, we will seek to obtain parental consent, for example, we will ask a parent, or someone with parental responsibility (i.e., someone who has the legal rights and responsibilities for a child that are normally afforded to parents), to sign a membership application form on behalf of the child.

For children aged 13 to 17 years, we will ask a parent, or someone with parental responsibility, to provide parental consent with the child, for example, to countersign a QPTC CIC Photography and Filming consent form with the child.

8. Roles and Responsibilities

QPTC CIC Directors

QPTC CIC directors must ensure that QPTC CIC complies with its legal obligations and is able to demonstrate compliance with the data protection principles and take appropriate technical and organisational measures to ensure that processing is carried out in line with the UK GDPR. This includes ensuring that the relevant organisational arrangements and resources are made available to manage internal data protection activities, and to ensure this policy is implemented and monitored.

QPTC CIC is not required by the ICO to appoint a Data Protection Officer. However, the directors will appoint a Data Protection Compliance Lead and ensure that person understands the data processing undertaken by QPTC CIC and is appropriately trained to enable them to undertake that role.

Data Protection Compliance Lead

The Data Protection Compliance Lead is Stephen Lee. They are responsible for:

- providing advice and guidance to staff and volunteers on data protection issues
- ensuring the provision of data protection training for all staff and volunteers and keeping training records
- arranging the completion of an annual audit/mapping exercise to assess compliance and identify whether there are any areas of vulnerability in the processing and security of personal data by QPTC CIC and report any remedial steps required to the QPTC CIC directors for appropriate and timely resolution
- reviewing our Privacy Notices regularly to ensure they remain up to date

- dealing with any suspected or known data breaches and reporting to and liaising and cooperating with the Information Commissioner's Office on any data breaches
- handling any subject access requests made to QPTC CIC, or any exercise by an individual of his/her rights
- regularly checking ICO news and guidance pages for updates.

The Data Protection Compliance Lead will keep records of privacy notices wording used, consents (where applicable) and any other relevant information related to processing of personal data.

QPTC CIC staff and volunteers

(Our volunteers include committee members, team captains, welfare officer, communications officer, tournament organisers, and others).

All direct employees of QPTC CIC and all volunteers working directly within the organisation are classed as data controllers.

All QPTC CIC staff and volunteers are responsible for:

- familiarising themselves with this Data Protection Policy and implementing it, with particular attention to data storage and security and retention periods
- ensuring they receive, create, maintain or delete records in accordance with this Data Protection Policy
- complying with the UK GDPR and other relevant data protection laws
- requesting help from the Data Protection Compliance Lead if they are unsure about any aspect of data protection
- not sharing data informally
- seeking and obtaining permission before taking photos or videos of individuals and before posting them in QPTC WhatsApp groups, social media platforms or our website
- attending data protection training if required by the directors
- reporting any actual or suspected data breaches as soon as possible to the Data Protection Compliance Lead.

ClubSpark Administrators

Administrators with access to Membership and Booking information must always sign out when they have finished doing anything in ClubSpark, e.g., booking a court.

9. Data Retention Periods

QPTC CIC must only keep personal data for as long as is necessary for our reasonable purposes. There is some flexibility around how long it can be kept, and retention periods will vary depending on the type of data and why it was collected in the first place. For example, we can retain member and employee data for a period after membership has ended or employment has terminated. For some types of records, the retention period will be determined by statutory requirements, while for others it is for QPTC CIC to determine. This balances legal compliance, operational needs, and respect for individuals' privacy.

Data records should be reviewed in accordance with the following retention schedule.

Retention Schedule

Record type	Retention period	Notes
Membership forms	1 year after the individual ceases to be a member	Unless needed for ongoing matters or legal requirement
Employment and training records (contracts, payroll, pension, disciplinary)	6 years after employment ends	Limitations Act Required for potential claims and HMRC compliance
Employee references provided by QPTC CIC	1 year after issue	To respond to queries; not needed long-term
Unsuccessful job applications and interview records	6 months	Limitations Act To defend against discrimination claims
DBS information	Up to 6 months after decision	Only retain certificate number and date; destroy full details promptly
Financial information (accounts, invoices, receipts)	6 years from end of financial year	HMRC requirement
Donations (records of donors, amounts)	6 years	Linked to financial records
Venue hire agreements and correspondence	6 years after expiry	Linked to financial records
Contracts with suppliers, agents and others	6 years after expiry or termination of contract	Limitations Act
Management Committee meeting minutes and governance records	Permanently	Required for historical archive
Emails produced or received (general correspondence)	2 years	Emails should be periodically permanently deleted, unless they are needed for ongoing matters or relate to a record type which requires a longer retention period
Images – photos and videos (including on QPTC Facebook and QPTC website)	2 years (NB. images on WhatsApp * cannot be deleted and therefore could remain forever)	As per our photography and filming consent forms
CCTV footage	15 days	Footage data is stored in case it is required by Police or another agency or authority following criminal activity or in relation to another incident or required in support of an insurance claim.
Complaints	6 years after resolution	Aligns with potential window for legal claims
Visitor records	6 years	For compliance and security
Accident books / forms	3 years after last incident entry or end of investigation	Health & Safety legislation requirement

	if later (or until child reaches 21 yrs if involving a minor)	RIDDOR
Safeguarding records	Kept for 35 years	Legislation requirement

* When an individual cancels or stops renewing their membership they should remove themselves from any QPTC WhatsApp groups they are in, and QPTC CIC will twice yearly remove past members.

Principles

- Minimisation: Only keep data necessary for the stated purpose.
- Secure storage: Records must be stored securely, with restricted access.
- Disposal: At the end of retention, records must be securely destroyed (shredded or permanently deleted).
- Review: Annual audit of records to ensure compliance.

Exceptions

Where records are subject to ongoing legal proceedings, investigations, or audits, they may be retained longer than the stated period.

10. Data Subject Access Request – procedure

Individuals have the right to ask whether we are using or storing their personal information. Individuals can ask us to receive a copy of their personal information. This is known as making a subject access request. All requests can be made by email to admin@qptc.co.uk

Requests should be passed to the Data Protection Compliance Lead as soon as possible. QPTC CIC will respond to the request within one month. A charge will not be made to the individual unless their request is judged to be manifestly unfounded or excessive.

The Data Use and Access Act 2025 clarifies the time limits for organisations to respond to subject access requests. It includes a “stop the clock” rule, allowing organisations to pause the response time if they need more information from the requester. Once they get the information they need, the response time continues. Organisations need to make reasonable and proportionate searches to find and retrieve the requested information, when responding to requests.

Staff and volunteers should not alter, conceal, block or destroy personal data once a request for access has been made. Staff and volunteers should contact the Data Protection Compliance Lead before any changes are made to personal data which is the subject of an access request.

11. Data breaches

A data breach is any occasion where personal data is lost, corrupted or altered without proper permission; or where it was damaged, destroyed or disclosed inappropriately, whether by accident or deliberately. This can include where someone accesses data or passes it on without proper authorisation, or if the data is made unavailable when encrypted by ransomware. Breaches can be the result of both accidental and deliberate causes, e.g., because of a cyber-attack, flood, fire or theft.

It is important that any actual or suspected data breaches are reported as soon as possible, so that risks can be assessed and mitigating actions taken. Breaches should be reported to the Data Protection Compliance Lead or, in their absence a director.

Certain types of data security breach (such as actual or potential loss, corruption or theft of data) must be reported to the ICO within 72 hours of QPTC CIC becoming aware of it. Where the breach is likely to present a high risk to an individual (for example if his/her financial or special category data has been compromised), they should be notified directly.

The ICO can be notified either by phone or online:

- phone: 0303 123 1113 Mon-Fri 9.00-4.30.
- online form is available: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach

Records of personal data breaches must also be kept, setting out:
a) the facts surrounding the breach
b) its effects; and
c) the remedial action taken.

12. Data Protection complaints

The Data Use and Access Act 2025 has introduced a requirement for organisations to have a data protection complaints handling process. If an individual is concerned that the way their information is used breaches the data protection legislation, they can make a complaint. They should follow the procedure in the QPTC CIC Compliments and Complaints Policy.

13. Data sharing

QPTC CIC will be transparent with all individuals about how we will use their data, and in most cases, individuals will be made aware of how and with whom their information will be shared, e.g., the Brighton & Hove Parks Lawn Tennis Association for members playing in the Parks League. However, there are certain circumstances where the law requires QPTC CIC to disclose data without the person's consent (e.g. to protect a person's life or in a critical safety situation).

Our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policy. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes.

Data Sharing Agreements

A data sharing agreement provides a framework to help organisations meet the requirements of the data protection principles. A data sharing agreement:

- helps all the parties be clear about their roles
- sets out the purpose of the data sharing
- covers what happens to the data at each stage
- sets standards.

There is no set format for a data sharing agreement; it will depend on the nature of the data, what is being shared, how and with whom.

14. ClubSpark

QPTC CIC has enlisted the services of a third party, ClubSpark Group Ltd, to provide the online court booking system for the club. They provide the software, the servers, and the booking system. They store data and provide the App security. Their relationship with QPTC CIC is as a Data Processor. ClubSpark provide their own privacy and data policy: https://clubspark.co/clubspark/Privacy

15. CCTV and images

An image of an individual is considered their personal data.

We operate CCTV (closed circuit television) surveillance systems on our premises with CCTV inside and outside the clubhouse, including cameras which are directed at all 6 tennis courts. We use CCTV for the prevention and detection of crime and for protecting the safety of individuals, or the security of premises.

QPTC members can view live court camera images through the members area of the QPTC website.

CCTV images are stored in the recorder for 15 days and are then over-wiped. The CCTV recordings can be accessed by the Facilities Manager (Mel Bowden). For additional information please see the QPTC CIC CCTV Surveillance System Policy & Procedures: Club Policies - Queens Park Tennis Club Brighton

Images also include photographs and videos. QPTC CIC staff and volunteers should only take and share photos and videos when you have agreement from everyone whose image will be taken. This includes photos and videos that will be posted in WhatsApp groups, on social media accounts (including QPTC's Facebook) and on the QPTC website.

Consent can be provided verbally by adults (18 years and over), or in writing using a QPTC CIC Photography and Filming Consent Form. With verbal consent, a log / record should be maintained with everyone's names and a date of when the photo or video were taken.

Photo and video images of children under 18 require signed parental consent.

16. QPTC Coaches

The tennis coaches at QPTC are self-employed and operate under a contract with QPTC CIC. Because they are self-employed, they are responsible for the personal data they process from their coaching customers, not QPTC CIC, regardless of whether those customers are also members of QPTC or are non-member players at QPTC. As self-employed professionals, they are Data Controllers themselves. If you are a customer of one of the coaches at QPTC and have a question about your personal data, please contact them directly.

17. Policy review

This policy will be reviewed every two years, or sooner if internal or external factors deem it necessary. We reserve the right to change this policy at any time without notice to you so please check regularly to obtain the latest copy.

18. Further information

Full details of the Data Protection Act:
Data Protection Act 2018

Information Commissioner's Office:
Information Commissioner's Office

UK GDPR guidance and resources:
UK GDPR guidance and resources | ICO

Advice for small and medium organisations:
Advice for small and medium organisations | ICO

Report a breach:
https://ico.org.uk/for-organisations/report-a-breach

Data Protection audit framework:
https://ico.org.uk/for-organisations/advice-and-services/audits/data-protection-audit-framework/

The Data Use and Access Act 2025:
https://www.gov.uk/guidance/data-use-and-access-act-2025-data-protection-and-privacy-changes

The Data Protection Network:
https://dpnetwork.org.uk/

Children and the UK GDPR:
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr/

Data Subject Access Request guide:
Data Subject Access Request Guide | Data Protection Network
Data Subject Access Requests – what are people entitled to? | Data Protection Network

Data sharing:
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/navigating-the-data-sharing-code/

19. Related documents

QPTC CIC CCTV Surveillance System Policy
QPTC CIC Compliments and Complaints Policy
QPTC CIC GDPR Data Audit 2026
QPTC CIC Photography and Filming Consent Forms
QPTC CIC Photography and Filming Policy
QPTC CIC Privacy Notices
QPTC Membership forms

20. Equality Impact Assessment

This Equality Impact Assessment (EIA) helps QPTC CIC to consider whether a policy discriminates or unfairly disadvantages people from a range of groups and helps us think through actions that can be taken to lessen impact and advance equality, diversity and inclusion.

Impact summary: summarise whether the proposed policy will have a disproportionate impact on any of the groups listed below and what actions if any will be taken.	
Age	Potentially positive.
Disability: Hearing impairment Visual impairment Physical disability Learning disability Mental health need	Potentially positive. This policy has not been adapted to an easy read version and as such may disadvantage some people with learning disabilities. This policy has not been adapted for and therefore disadvantages people that are visually impaired.
Gender reassignment (incl. trans & non-binary)	Potentially positive.
Marriage and civil partnership	Potentially positive.
Pregnancy and maternity	Potentially positive.
Race: People from diverse ethnic backgrounds; Refuges & asylum seekers; People with English as an additional language	Potentially positive. This policy has not been adapted to an easy read version and as such may disadvantage some people with English as an additional language.
Religion or belief	Potentially positive.
Sex - men, women and intersex	Potentially positive.
Sexual orientation	Potentially positive.
People with (unpaid) caring responsibilities	No impact identified.
People from lower socio-economic backgrounds and people living in areas facing deprivation	No impact identified.
People with low levels of English	No impact identified. This policy has not been adapted to an easy read version and as such may disadvantage some people with low levels of English.
Intersectionality (include relevant information relating to the intersection of any of these protected groups)	No impact identified.

Policy control sheet

Policy title	QPTC CIC Data Protection Policy
Version number	V1
Policy owner	Name: Stephen Lee Designation: QPTC CIC Data Protection Compliance Lead
Target audience	All Queens Park Tennis Club members, Guests of members, Parents and legal guardians of child members, Committee members, Directors, Coaches, Staff, Volunteers, Clubhouse key holders, Clubhouse visitors (including private hires), Contractors, Suppliers, Pay and Play users, and other customers
Document status	FINAL
Date approved	3.5.2026
Approved by	QPTC CIC directors and management committee
Effective date	3.5.2026
Date of last review	N/A
Date of next review	3.5.2027

Amendment history

Version no. & date created	Author	Summary of changes made
30.4.26	Mark Cull	New policy. Incorporated changes introduced by the Data Use and Access Act 2025.