Queens Park Tennis Club CIC
CCTV Surveillance System 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, Staff, Volunteers, Coaches and other Contractors, Staff, Clubhouse key holders, Clubhouse visitors (including private hires), Suppliers, Pay and Play users and other customers.

Contents:

1. Policy statement

Queens Park Tennis Club CIC (QPTC CIC) is committed to protecting your personal information and your overall safety and security in relation to your time in our facilities.

At Queens Park Tennis Club we operate a CCTV (closed circuit television) surveillance system monitoring our premises 24 hours a day. We have CCTV inside and outside the clubhouse and cameras which are directed at all 6 tennis courts. All CCTV surveillance is automatically recorded. Any audio capabilities in our system are switched off by default.

We have considered the need for using CCTV and have decided it is necessary for the prevention and detection of crime and for protecting the health and safety of individuals, and the security of our premises and assets. We will not use the system for any incompatible purposes, and we conduct regular reviews of our use of CCTV to ensure that it is still necessary and proportionate.

This CCTV system and the images produced by it are controlled by QPTC CIC who is responsible for how the system is used under the UK GDPR and Data Protection Act 2018.

The QPTC CIC Data Protection Compliance Lead is responsible for ensuring that standards are set, procedures are put in place to meet these standards, and that our CCTV surveillance system complies with the Information Commissioner's Office (ICO) guidance and other legal obligations. QPTC CIC is registered as a Data Controller with the ICO,

The images produced by the equipment will as far as possible be of a quality that is effective for the purpose(s) for which they are intended. By entering onto our premises, you consent to your image being recorded and reviewed and waive any and all claims in relation to same.

2. Data Protection concepts

Our responsibilities in terms of accountability

QPTC CIC must take a data protection by design and default approach and perform a Data Protection Impact Assessment (DPIA) for any processing that is likely to result in a high risk to individuals. This includes:

- processing special category data.
- monitoring individuals at a workplace.

We have determined that our use of surveillance is appropriate in our circumstances, having given due consideration to the reasonable expectations of the individuals whose personal data are processed and the potential impact on their rights and freedoms.

Our responsibilities in terms of transparency

We have appropriate restrictions in place on viewing and disclosing images for those operating the system.

We have signs that accompany our surveillance system that are clearly visible and readable, explaining that its use is in operation, so that people who are in an area where our surveillance system is in operation are aware that they are being recorded. We display signs inside and outside the clubhouse and by the entrance gates to our tennis courts. Our signage includes details of the organisation operating the system (QPTC CIC), the purpose

for using the system and who to directly contact about its use. We include as a minimum basic contact details such as a website, telephone number or email address.

Lawful basis for processing or using personal data

QPTC CIC can only use an individual's personal data if we have a "lawful basis" for doing so. There are six lawful bases for processing personal data set out in the UK GDPR, in relation to our CCTV surveillance system, we use 'Legitimate Interests'.

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.

Our Legitimate Interests are for the prevention and detection of crime or disorder, apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings), interest of the Health and Safety of individuals, protection of public health, and the security and protection of our property and assets, and to ensure compliance with our policies and procedures.

The Data Use and Access Act (DUAA) 2025 introduced changes to data protection law, including a new lawful basis of processing – 'Recognised Legitimate Interests'. Schedule 4 of the DUAA Act sets out the conditions that an organisation needs to meet when relying on the new Recognised Legitimate Interests lawful basis for processing. One of these conditions is Crime: this allows an organisation to use personal information where this is necessary for the purposes of:

- detecting, investigating or preventing crime; or
- apprehending or prosecuting offenders.

3. Data Protection Impact Assessment

In April 2026 we reviewed the ICO guidance about the types of risks posed by surveillance systems and the list of processing operations for which the ICO would require us to complete a Data Protection Impact Assessment (DPIA) as the processing operations would be 'likely to result in high risk' - none of those apply to QPTC CIC. We are clear about the nature, scope, context and purposes of the processing, which is for the prevention and detection of crime or disorder, apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings), interest of the Health and Safety of individuals, protection of public health, and the security and protection of our property and assets, and to ensure compliance with our policies and procedures; and on that basis we have determined that it is not necessary to carry out a DPIA now, but we will keep this under review.

4. Live images

Not only does our CCTV surveillance system record our 6 tennis courts for health and safety and security purposes, but it also live streams footage of all six tennis courts over the internet, which can be viewed in real-time by QPTC members through the restricted

members area of the QPTC website which requires a username and password. The live streaming of images of identifiable individuals is subject to the requirements of the UK GDPR and Data Protection Act 2018.

5. Toilets and changing areas

The cameras do not infringe on sensitive areas - there are no CCTV cameras inside rooms where people would expect a high degree of privacy such as toilets and changing areas.

6. Employees, Contractors and Volunteers

The QPTC facilities are also spaces where our employees and contractors work and where people volunteer and carry out tasks. The CCTV surveillance system has not been installed to monitor staff and volunteers in the workplace performing their day-to-day roles. However, as with all users of our facilities, the surveillance system is for everyone's health and safety and security.

If an employee, contractor or volunteer has any concerns about our use of CCTV they can raise a concern with their line manager or make a complaint by following the complaints procedure detailed in the QPTC CIC Compliments and Complaints Policy.

When new employees, contractors and volunteers are recruited they should be informed and consulted about the operation of our CCTV surveillance system.

7. Retention period

All images are digitally recorded and stored securely within the system's hard drives for 15 days and are then over-wiped. The CCTV recordings can be accessed by the Facilities Manager.

8. Exercising your rights under UK GDPR

Under data protection law, individuals have certain rights, such as the right of access, erasure or restriction. The right of access gives individuals the right to obtain a copy of their personal data from us and in a timely manner, including CCTV images which contain their personal data.

Individuals can make a subject access request verbally or in writing or can follow-up a verbal request with a written one. They should provide sufficient details to identify the section of footage they are concerned with.

Upon receipt of the request, the Facilities Manager and our Data Protection Compliance Lead will decide whether the information we hold is personal data and, if so, whose personal data it is. They will determine whether disclosure is appropriate and whether there is a duty of care to protect the images of any third parties. If the duty of care cannot be discharged, then the request can be refused.

If we are unsure whether a request is valid, we will check with the individual that we have understood their request. This can help avoid later disputes about how we have interpreted it and prevents delays. Individuals who request access must provide us with supporting

details, such as a photo, date or time, that allows us to identify them as the subject of the information and to help locate the personal data on our system efficiently.

We are required to provide the data subject with a copy of all the information caught by the request that constitutes their personal data, unless an exemption applies. A written response will be made to the individual, giving the decision (and if the request has been refused, giving reasons) within 31 days of receipt of the request.

If the request has been approved, we will supply them with a copy of the information in a permanent form or, if they agree, allow or arrange for them to view the information. If an individual refuses an offer to view the footage or they insist on a copy of the footage, then we will do whatever is reasonable in the circumstances to provide them with a copy of this information.

We will provide information promptly and within one month of receiving the request. Under the UK GDPR, we can extend the time to respond by a further two months if the request is complex or we have received several requests from the individual. Providing information promptly is important because our retention period for surveillance footage is 15 days and then it is routinely deleted. In such circumstances it is good practice to prevent the premature deletion of any information that falls within the scope of a request.

Providing an individual with a transcript of the visual information contained in the footage is not enough to comply in most circumstances. This is because a transcript, or even a still photograph in some circumstances, is unlikely to fully communicate all the contextual information within the footage that could be considered the data subject's personal data.

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

For more information about how individuals can exercise their rights, please see the QPTC CIC Data Protection Policy: Club Policies - Queens Park Tennis Club Brighton

9. Disclosure of information to third parties from our surveillance system

Access to, and disclosure of, the images recorded by our CCTV surveillance system is restricted and carefully controlled. This ensures that the rights of individuals are preserved, and the continuity of evidence remains intact should the images be required for evidential purposes e.g. a Police enquiry or an investigation being undertaken as part of an internal procedure.

We will ensure that any access to and disclosure of information to third parties from our surveillance system is controlled and that the disclosure itself is consistent with the purpose(s) for which such images were collected. For example, in most cases it is appropriate to disclose video surveillance information to law enforcement when the purpose of the system is to contribute to the prevention and detection of crime. Unless a court order applies, this is not a legal requirement and is often voluntary. But this could be QPTC CIC proactively disclosing CCTV footage of a crime taking place on our premises, to the police.

As the operator of the surveillance system, any decisions about disclosure are our responsibility. We have discretion to refuse any request unless there is an overriding legal obligation. For example, a court order.

Once information is disclosed to a third party, they become the controller for the copy they hold. It is their responsibility to also comply with the UK GDPR and the DPA 2018 for any further disclosures. It is also important that any method of disclosing information is secure. This is to ensure the footage is only seen by the intended recipient and not lost in transit or unintentionally distributed further.

10. Redacting information about third parties

In the context of video surveillance, responding to the right of access may involve providing information that relates both to the requester and another individual. Our obligations are to provide a copy of the information about the requester rather than a complete version of footage. But also, to ensure doing so does not adversely affect the rights and freedoms of others. Therefore, we may have to consider seeking the consent of third parties where reasonable or alternatively removing or redacting footage. We will consider the nature and context of the footage to determine the level of harm that may arise from choosing not to redact. In practice, we will approach each request for information on a case-by-case basis, and make a reasonable determination based on the circumstances.

For example, from a traditional CCTV system, available techniques could include blurring, masking, or using a solid fill to completely obscure parts of the footage. To do this, we may need to use specialist software to redact visual data.

11. Operational management roles & responsibilities

We ensure that access to footage is restricted only to authorised individuals. Day to day operational management of our CCTV surveillance system is the responsibility of our Facilities Manager, Mel Bowden.

The Facilities Manager is responsible for:

- notifying the Data Protection Compliance Lead of any Subject Access Requests received.
- working with the Data Protection Compliance Lead around any subject access requests and decide together whether a subject access request is valid.
- keeping a log of any verbal requests to ensure a satisfactory record and audit trail.
- providing footage to individual requesters or law enforcement in a commonly used video file format.
- where information is disclosed to a third party, that the method is secure and it is safely delivered to the intended recipient.
- keeping a record of any data sharing, specifically the date of the disclosure along with details of who we have provided the information to (the name of the person and the organisation they represent) and why they required it.
- regularly checking that the date and time stamp recorded on images is accurate (e.g., when the UK switches between summer and winter time).

Our Data Protection Compliance Lead is responsible for ensuring that:

- all relevant staff and volunteers have read and understood this policy and know who to contact if someone makes an enquiry about our CCTV surveillance system or a subject access request.

- our Facilities Manager is aware of the rights that individuals have, and can recognise a request from individuals to access, erase or restrict personal data, and can help progress these requests efficiently.
- we have internal procedures for the handling of requests. This includes keeping a log of the requests we receive and how we dealt with them within the statutory timescales.
- we have procedures in place to help locate the requester's information. This includes using the date, time and location where the footage was captured.
- any disclosure of information to third parties from our surveillance system is consistent with the purpose(s) for which we set up the system.
- we have a surveillance system that can produce good, clear, quality images, and that the quality of the information collected is also maintained throughout the recording process.
- our surveillance system is designed to easily locate and extract personal data in response to subject access requests.
- the Facilities Manager is trained to use professional software that can redact visual data.
- we periodically review our system's effectiveness to ensure that it is still doing what it was intended to do. If it does not achieve its purpose, we will stop the processing until we have modified the system accordingly.
- we regularly assess (as a minimum, annually) whether the use of any camera and the whole CCTV surveillance system continues to be justified, necessary and proportionate.
- we periodically review whether we need to complete a Data Protection Impact Assessment, particularly if we are about to make changes to the CCTV surveillance system that will impact on individuals' rights and freedoms.
- we have data sharing agreements in place where appropriate, if we need to share information on an ad hoc or routine basis.

12. Further information

Video surveillance (including guidance for organisations using CCTV) | ICO

Data protection impact assessments for surveillance cameras - GOV.UK

13. Related documents

QPTC CIC Compliments and Complaints Policy
QPTC CIC Data Protection Policy
QPTC CIC Membership forms

14. Procedure checklist

Checked (Date)	By	Date of next review
If our system is processing footage of identifiable individuals and is processing personal data, we have registered as a controller and submitted a relevant data protection fee to the Information Commissioner's Office (ICO). We have also recorded the next renewal date.	Mark Cull	24.4.26
There is a named individual who is responsible for the operation of the system.	Mark Cull	24.4.26
Prior to processing we have clearly defined the problem we are trying to address. We regularly review our decision to use a surveillance system.	Mark Cull	24.4.26
We have identified and documented an appropriate lawful basis for using the system, taking into consideration Article(s) 6, 9 and 10 of the UK GDPR and relevant Schedules of the DPA 2018.	Mark Cull	24.4.26
Our system produces clear images which we can easily disclose to authorised third parties. For example, when law enforcement bodies (e.g., Police) require access to investigate a crime.	Mark Cull	24.4.26
We have positioned cameras in a way to avoid any unintentional capture of private land or individuals not visiting the premises.	Mark Cull	24.4.26
There are visible signs showing that CCTV is in operation. Contact details are displayed on the sign(s) if it is not obvious who is responsible for the system.	Mark Cull	24.4.26
We securely store images from this system for a defined period and only a limited number of authorised individuals may have access to them.	Mark Cull	24.4.26
Our organisation knows how to respond to individuals making requests for copies of their own images, or for images to be erased or restricted. If unsure the controller knows to seek advice and guidance from the Information Commissioner's Office (ICO) as soon as a request is made.	Mark Cull	24.4.26

15. 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	
Disability: Hearing impairment Visual impairment Physical disability Learning disability Mental health need	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)	
Marriage and civil partnership	
Pregnancy and maternity	
Race: People from diverse ethnic backgrounds; Refuges & asylum seekers; People with English as an additional language	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	
Sex - men, women and intersex	
Sexual orientation	
People with (unpaid) caring responsibilities	
People from lower socio-economic backgrounds and people living in areas facing deprivation	
People with low levels of English	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)	

Policy control sheet

Policy title	QPTC CIC CCTV Surveillance System 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, Staff, Volunteers, Coaches and other Contractors, Staff, Clubhouse key holders, Clubhouse visitors (including private hires), Suppliers, Pay and Play users and other customers.
Document status	FINAL
Date approved	
Approved by	
Effective date	
Date of last review	N/A
Date of next review	

Amendment history

Version no. & date created	Author	Summary of changes made
24.4.26	Mark Cull	New policy.