SUFFOLK
LAWN TENNIS ASSOCIATION

INFORMATION GOVERNANCE POLICY

Approved: 28th March 2024

For review by: March 2027

INTRODUCTION

Information governance is the process by which an organisation obtains and provides assurance that it is complying with its legal, policy and moral responsibilities in relation to the processing of information. Suffolk Lawn Tennis Association (SLTA) considers that the following areas fall under the scope of information governance:

- Data protection
- Information Security
- Information access[1]
- Knowledge and Information Management (including record management and data quality)
- Confidentiality.

This policy defines Suffolk Lawn Tennis Association's (SLTA) approach to information governance. It provides assurance that our practices comply with legislation and our business requirements, and that information risks are appropriately recognised and managed. The aims of this policy are:

- To ensure that information (including information about identifiable people and other confidential information) are:
  - Held securely
  - Obtained fairly and lawfully
  - Recorded and managed accurately and reliably
  - Used effectively and ethically
  - Shared and disclosed appropriately and lawfully.
- To ensure that information risks are identified and managed,
- To ensure that all volunteers, staff and contractors recognise and meet their own responsibilities and accountabilities in relation to the processing of information, and
- To maximise the value of SLTA's organisational information assets, through their effective and lawful management.

[1] The Freedom of Information Act does not apply as SLTA is not a public authority

Policy Statement

Information is vital to SLTA's role as a Lawn Tennis Association (LTA) County Association. Only by the effective obtaining, use and sharing of information can SLTA meet its purposes. Failure to adequately protect and manage information would create an unacceptable risk to the privacy of people who contribute to providing, and who use its services; as well as to the privacy of other people whose information SLTA may have access to, obtain and use. Failure to identify and meet the obligation of confidentiality may also create significant risks to the effectiveness of SLTA's governance, the rights and legitimate interests of users and providers of services, and public trust in tennis as a regulated sport.

All volunteers, staff and contractors of SLTA are required to comply with this policy framework and the specific policies set out below.

DATA PROTECTION POLICY

Purpose

This policy defines SLTA's approach to processing personal data. It provides assurance that our practices comply with legislative and business requirements.

Policy Statement

SLTA will process personal data in accordance with the requirements of data protection law including the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR). The processing of personal data is vital to SLTA's role as an LTA County Association. The effective obtaining, use and sharing of personal data is often necessary for SLTA to meet its purposes. Failure to adequately protect and manage personal data would create an unacceptable risk to the privacy of people who contribute to providing, and who use its services; as well as to the privacy of other people whose personal data SLTA may have access to, obtain and use.

Scope

This policy applies to all processing of personal data by or on behalf of SLTA. This includes the processing of personal data relating to people who use the services SLTA provides directly and through contractors; staff; volunteers; partners; patrons; and any other persons whose personal data it processes. The scope of this policy includes the processing of personal data by third parties acting on behalf of SLTA.

Definitions

Personal data is any information processed by SLTA which identifies and relates to a living person. This includes information which directly identifies a living person, but also to information which is not directly identifiable but which could be linked back to the person by reference to other information held by SLTA, is likely to come into the possession of SLTA, or which SLTA has powers to obtain. It does not include anonymous or anonymised data.

Special category personal data is personal data which reveals or relates to physical or mental health (including health and care needs, or treatment), race or ethnic origin,

political opinions, religious or philosophical belief, trade union membership, sex life or sexual orientation, and criminal convictions.

Processing means any operation, action on, or interaction with personal data, whether carried out by a person or by automated means. Processing includes, but is not limited to: access to, obtaining, recording, organisation or structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, sharing, publication, restriction, erasure or destruction of personal data.

Data subjects are the people to whom personal data relates.

Privacy notices are information that is communicated to data subjects to inform them of how and for what purpose(s) their personal data will be processed by SLTA, and which provide them with further information prescribed under data protection law, including information of the security and retention of the data, and on the data subject's rights.

Data Protection Principles

In accordance with data protection law, SLTA will ensure that all processing of personal data is carried out in accordance with the principles relating to the processing of personal data, which require that personal data shall be:

- Processed lawfully, fairly and in a transparent manner.
- Collected only for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date.
- Kept in a form which permits the identification of data subjects for no longer than is necessary.
- Kept secure, with appropriate measures to protect against unauthorised or unlawful processing, accidental loss, destruction or damage.

SLTA will maintain appropriate records to demonstrate compliance with the data protection principles.

Lawful bases for processing

SLTA will maintain registration with the Information Commissioner's Office[2].

It will only process personal data or special category personal data where it has identified that a lawful basis for doing so is engaged under data protection law. It will maintain records of the lawful bases relied upon for the processing of personal data.

Most commonly, it will use personal information in the following circumstances:

- Where it needs to perform the contract entered into with a data subject.
- Where it needs to comply with a legal obligation.
- Where it is necessary for legitimate interests pursued by SLTA or a third party and the data subject's interests and fundamental rights do not override those interests.
- SLTA may also use personal information in the following situations, which are likely to be rare:
  - Where it needs to protect the interests of the data subject or someone else's interests.
  - Where it is needed in the public interest.

There has to be further justification for collecting, storing and using special category personal data. SLTA may process it in the following circumstances:

- In limited circumstances, with the data subject's explicit written consent.
- Where it needs to carry out our legal obligations or exercise rights in connection with employment.
- Where it is needed in the public interest, such as for equal opportunities monitoring.

[2] https://ico.org.uk

- Where it is necessary to protect the data subject or another person from harm.

Less commonly, SLTA may process this type of information where it is needed in relation to legal claims or where it is needed to protect the data subject's interests (or someone else's interests) and they are not capable of giving consent, or where they have already made the information public.

In general, SLTA will not process particularly sensitive personal information about a data subject unless it is necessary for performing or exercising obligations or rights in connection with their role. On rare occasions, there may be other reasons for processing, such as it is in the public interest to do so

Consent

Consent is one lawful basis for processing personal data. Explicit consent is one lawful basis for processing special category personal data. For consent to be valid, it must be informed and freely given. Consent must be indicated by a positive action, and cannot be implied from failure to respond, object or opt out. Consent may be withdrawn at any time and SLTA will ensure that withdrawing consent is as easy as giving consent.

SLTA will not rely upon consent as the only lawful basis for processing for the purpose of exercising its legitimate functions. Where SLTA does rely upon consent as a lawful basis for processing, it will maintain records as evidence of consent.

SLTA does not need the data subject's consent to use special categories of personal data in accordance with this policy to carry out its legal obligations or exercise specific rights in the field of employment law.

SLTA does not need a data subject's consent where the purpose of the processing is to protect them or another person from harm, and if there is a reasonable belief that they need care and support, are at risk of harm and are unable to protect themselves.

In the limited circumstances where consent to the collection, processing and transfer of personal data for a specific purpose has been obtained, the data subject has the right to withdraw consent for that specific processing at any time by contacting secretary@suffolklta.uk. This will halt the process of the data for the purpose or purposes that consent was originally given, unless there is another legitimate basis for doing so in law.

Other requirements of data protection law

SLTA will also comply with the other requirements of data protection law, which include (but are not limited to):

Complying with the rights of data subjects.

SLTA will ensure that there are processes in place to comply with the rights of data subjects. These include:

Right of data access: SLTA will have a process to manage and respond to requests from data subjects for access to their own personal data and for information as to how and for what purpose(s) it is being processed by SLTA.

Right to erasure ('right to be forgotten'), right to restriction of processing, and right to object to processing: SLTA will manage and respond to requests from data subjects that SLTA should erase their personal data. SLTA will manage and respond to requests from data subjects for the restriction of processing of personal data concerning them in specified ways or in specific circumstances. SLTA will manage and respond where a data subject objects to the processing of their personal data by SLTA, on grounds relating to their personal situation.

These processes will recognise that these rights are qualified, and may be refused where SLTA needs to continue processing the personal data for legitimate reasons (with a lawful basis), including where it is necessary and in the public interest to do so for the exercise of its functions or in relation to legal claims.

Right to rectification: SLTA will manage and respond to requests from data subjects for the rectification of inaccurate personal data concerning them. SLTA will also respond to requests to suspend the processing of personal information by a data subject if, for example, they want its accuracy to be established or the reason for processing it.

Data subjects will not have to pay a fee to access their personal information (or to exercise any of the other rights) although SLTA may charge a reasonable fee if a request for access is clearly unfounded or excessive or it may refuse to comply with the request in such circumstances.

SLTA may need to request specific information from the data subject to confirm their identity and right to access the information (or to exercise any of the other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Data protection by design and default, and data protection impact assessment (DPIA).

SLTA will ensure that any new process or change which is likely to result in a high risk to privacy, or to the rights and freedoms of data subjects, is first subject to a DPIA. This DPIA will include steps to establish the lawful basis for processing, and to understand and mitigate the likely risks. The DPIA shall also ensure that the processing of personal data is minimised, and that appropriate technical and organisational measures are integral to the design and operation of systems and processes that involve processing of personal data.

Notification of data breaches

SLTA will ensure that suspected data protection breaches are investigated, and that actual breaches are reported to the Information Commissioner's Office, and notified to data subjects, as required under data protection law.

Change of purpose

SLTA will only use the data subject's personal information for the purposes for which it was collected, unless it reasonably considers that use for another reason is required,

and that reason is compatible with the original purpose. If it needs to use the data subject's personal information for an unrelated purpose, SLTA will notify the data subject and will explain the legal basis which allows it to do so.

Please note that SLTA may process the data subject's personal information without their knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

If personal data is not supplied

If certain data is not provided by a data subject when requested, SLTA may not be able to perform the contract entered into with them, or provide the services offered to them; or it may be prevented from complying with legal obligations such as to ensure people's health and safety.

This policy should be read alongside the associated policies contained in this document.

INFORMATION SECURITY POLICY

Purpose

The overall purpose of the policy is to provide an overview of SLTA's information security requirements. They are also relevant as evidence of established information security practices during internal or external audit processes. Relevant sections of the policy may also be used as a reference point in negotiating or agreeing contracts with external suppliers. The measures and controls detailed within the policy set the security goals within SLTA to achieve compliance with ISO27001[3].

Scope

The policy applies to all volunteers, staff and contractors working with SLTA in whatever capacity. The policy complies with the requirements of widely recognised good information security practice. It will:

- Assist volunteers, staff and contractors to apply the correct level of security control to their day to day activities in line with good practice and applicable regulation and legislation.
- Assist with the development and commissioning of new processes and systems by detailing the required security settings and standards.
- Be formatted, controlled and distributed in line with SLTA's requirements.

Policy Statement

As an LTA County Association, SLTA aims to demonstrate the same standards of information security as it expects of partner organisations and services.

The importance of information security Information can be defined as useful data for a particular analysis, decision or task. Information must always be protected appropriately irrespective of how it is stored, presented or communicated. The main aims of information security are to preserve:

[3] The international standard for information security, addressing people processes and technology

- ***Confidentiality:*** ensuring that information is accessible only to those who are authorised to have access.
- ***Integrity:*** safeguarding the accuracy and completeness of information and processing methods.
- ***Availability:*** ensuring that authorised users have access to information when needed.

It also aims to support the requirements of:

- ***Accountability:*** accounting for the actions of individuals by monitoring their activities.
- ***Non-Repudiation:*** legally acceptable assurance that transmitted information has been issued from and received by the correct, appropriately authorised, individuals.

SLTA has a responsibility to securely manage its information assets, the information made available to it by providers and the people who use providers' services, as well as that provided by its own volunteers, staff, contractors and business partners. SLTA has a responsibility to protect that information from unauthorised disclosure, loss of integrity or loss of availability. All parts and agents of the organisation are responsible for making sure that information is protected adequately in accordance with this policy.

SLTA recognises the sensitive nature of some of the information that the organisation holds and processes, and the potential harm that could be caused by security incidents affecting this information. Security matters are considered as a high priority in making business decisions to ensure that SLTA allocates sufficient human, technical and financial resources to information security management

SLTA will take appropriate action in response to all violations of Security Policy.

The security efforts will be:

- ***Coordinated:*** security measures will be based on a common framework provided by the policy, and everyone working with SLTA will be involved in maintaining compliance with the security policy.
- ***Proactive:*** SLTA will detect, identify and manage vulnerabilities, threats, and security gaps to prevent security incidents as far as it can.
- ***Supported at the highest level:*** the management committee is actively committed to information security and gives full support to implementing the required security controls that are identified through a continuous risk assessment process.

This policy should be read alongside the associated policies contained in this document.

KNOWLEDGE AND INFORMATION MANAGEMENT POLICY

Purpose

This policy defines SLTA;s approach to knowledge and information management. It provides assurance that our practices comply with legislation and business requirements. It sets out a framework under which specific records management policies and procedures exist. This ensures that good practice to control records created internally or received from external sources is applied. It also provides clarity on the roles, responsibilities and accountabilities to follow the policy requirements.

Policy statement

Records provide vital evidence of decisions, activities and transactions. They are also essential in ensuring that SLTA meets legislative and regulatory requirements. SLTA is continually developing robust practices and processes to meet these requirements. Effective records management:

- Encourages improvement, innovation and sustainability
- Defines standards to ensure a consistent approach to records management
- Ensures that the integrity of records is maintained
- Protects sensitive information while still enabling data sharing with partners
- Improves efficiency and effectiveness by promoting ‘digital first’ and by managing and disposing of records once they no longer have a value.

The intention is that records are:

- Captured and stored in the right place
- Authentic so SLTA is confident that records are accurate
- Accessible in a timely way, by those who need or have a right to see them
- Protected from unauthorised deletion, changes or access
- Disposed of appropriately once they are no longer required.

Records should be held, wherever possible, in electronic format.

Scope

This policy principally applies to business related information contained within SLTA records that are held in offices (including home offices) and on SLTA systems. The policy applies to records in any format, for example electronic files, database entries, paper files, audio and video recordings. Although paper copies of records are not classed as records, the information they contain must be stored and managed in a way that prevents unauthorised access to the information that they contain.

This policy also applies to records stored by contracted third party organisations holding or processing SLTA business information. It applies to anyone who creates or has access to information stored in SLTA systems or offices (including home offices).

Definitions

Records are a valuable asset and must be managed in a way that recognises this. A record is information created, received and/or maintained as evidence by SLTA in its pursuance of legal obligations or business transactions, regardless of format. Records serve to detail SLTA's functions, policies, decisions, procedures or operations. Copies of records, or parts of them, are not records. Templates and blank forms are not records until completed.

Records management is the practice of managing the records of an organisation throughout their life cycle, from creation or receipt to their eventual disposal or transfer to permanent storage.

The principle of robust records management policies, procedures and practices means SLTA will:

- Meet legal responsibilities
- Manage records in line with recognised best practice
- Manage records with a consistent approach to eliminate variation
- Be able to find and analyse records easily
- Be confident that records are reliable and accurate
- Prevent loss or unauthorised access of records

- Store records securely
- Only store records whilst there is a business need
- Reduce paper storage
- Save time and money
- Make judgements based on accurate records.

An **Information asset** is a record or group of records, defined and managed as a single unit.

An ***information asset register*** describes SLTA's information assets. It details their owner, use, format, sensitivity, retention period, storage location and whether they contain confidential personal data.

The SLTA Secretary is responsible for:

Planning

- Maintaining an accurate Information Asset Register
- Inducting new users of SLTA information systems

Creation and capture

- Managing a system of naming electronic records
- Managing a system for paper and handwritten records
- Ensuring paper records are scanned and saved electronically
- Ensuring best practice when creating electronic records
- Ensuring emails and other messages that are SLTA records are retained/stored appropriately

Storage, maintenance and access

- Controlling access to records management systems by keeping a register of those with official email addresses entitled to access specific information and platforms
- Ensuring that sensitive or confidential information is held securely by those who are entitled to access it
- Managing records within shared systems, including the Cloud
- Sharing records

- Operating a system of version control
- Storing and maintaining paper records

Retention, review and disposal

- Identifying retention periods for categories of records based on business need and legislative requirements
- Defining which records need preserving and the procedures associated with this
- Ensuring that records no longer needing to be retained are disposed of timeously and safely based on business need and legislative requirements.

This policy should be read alongside the associated policies contained in this document.