# Data Protection Policy

---

This Data Protection policy sets out the commitment of Bourne & District Lawn Tennis Club (the Club) to protecting personal data and how we implement that commitment with regards to the collection and use of personal data.
The Data Protection Act 1998 ("the Act") governs the processing of personal data of identifiable living individuals. The definition of processing under the Act is very broad and covers actions such as obtaining, recording, storing, carrying out operations and destruction. It is very difficult to envisage any action involving data that is not covered.
"Data" is defined as including information that is processed automatically, recorded with the intention that it should be processed automatically and recorded in a relevant filing system or as part of an accessible record. A relevant filing system is one in which manual files have the same or similar ready accessibility as a computerised filing system. Therefore, endless unorganised files stacked in a basement would probably not be covered by the Act as a relevant filing system.

Whether the processed data is personal is determined by reference to the data itself or from the data and other information in possession of or likely to come into the possession of a data controller. Examples include an individual's name, address, national insurance number, photographs, CCTV images, blood samples and DNA samples.

There is an additional category of sensitive personal data which is defined as being data relating to racial or ethnic origin, political opinions, religious and other beliefs, trade union membership, physical and mental health or condition, sexual life, commission or alleged commission of an offence and proceedings relating to such an offence. All such data can only be processed in accordance with the Act and its principles.

The conditions for dealing with sensitive personal data are more stringent than for personal data. Persons that are responsible for determining the purposes for which and manner in which data is processed are known as data controllers. Individuals who are the subject of the personal data are known as data subjects. The data protection legislation is governed by the Information Commissioner.
**The Club is committed to:**

- Ensuring that we comply with the eight data protection principles, as listed below;
- Meeting our legal obligations as laid down by the Data Protection Act 1998
- Ensuring that data is collected and used fairly and lawfully.
- Processing personal data only in order to meet our operational needs or fulfil legal requirements.
- Taking steps to ensure that personal data is up to date and accurate.
- Establishing appropriate retention periods for personal data.
- Ensuring that data subjects' rights can be appropriately exercised.
- Providing adequate security measures to protect personal data.
- Ensuring that a nominated officer is responsible for data protection compliance and provides a point of contact for all data protection issues.
- Ensuring that all club officers are made aware of good practice in data protection.
- Providing adequate training for all staff responsible for personal data.

- Ensuring that everyone handling personal data knows where to find further guidance.
- Ensuring that queries about data protection, internal and external to the club, are dealt with effectively and promptly.
- Regularly reviewing data protection procedures and guidelines within the club.

**Data Protection Principles**

Under Schedule 1 of the Act there are eight principles under which data controllers must process data. These state that personal data must be:

- Processed fairly and lawfully;
- 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;
- Adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- Accurate and, where necessary, kept up to date; and
- Processed in accordance with the rights of data subjects under this Act.

Additionally:

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

**Conditions for processing personal data**

In order to process personal data lawfully the data controller must ensure that one of the conditions in Schedule 2 of the Act is met. In general, the consent of the data subject is required unless one of the other circumstances is relevant. These include scenarios such as where data is processed in order to complete a contract to which the data subject is a party and where the processing is necessary for the data controller to comply with a legal obligation.

**Conditions for processing sensitive personal data**

In addition to the conditions of Schedule 2, when dealing with sensitive personal data one of the conditions of Schedule 3 must be satisfied. Here the explicit consent to the processing of the personal data is required unless one of the other specified circumstances exists. These include where the processing is necessary for complying with employment law obligations and where the information has been deliberately made available to the public by the data subject.

**Rights of Individuals**

Sections 7 to 14 of the Act grant individuals a number of rights in relation to personal data held about them by others.

- Individual has the right to have access to personal data held about them. As part of this right they are entitled to be informed that personal data is being processed, a description of the personal data, the purpose for which it is being processed and others to whom the information may have been disclosed. Generally, this right can only be asserted in writing and after payment of the prescribed fee, currently £10. The data controller has 40 days in which to comply with the request and it is unlawful to alter the data before complying.
- Individuals have the right to prevent processing of their personal data where the processing is likely to lead to personal damage or distress.
- The individual must show that the damage or distress is substantial, allow a reasonable time limit for the processing to cease and the application must be made in writing to the data controller. This right is not available where data is processed under any of the first four circumstances of Schedule 2, which includes when the data subjects consent was given.
- Individuals have the right to prevent data being processed for the purposes of direct marketing. The objection must be made in writing and the data controller must comply as soon as possible. Individuals have the right to require a data controller to ensure that no decision which significantly affects the individual is based solely on the processing by automatic means of their personal data. Examples given by the Act of such decisions include the creditworthiness, reliability or conduct at work of employees.
- Individuals can apply to court to have the data controller rectify, block, erase or destroy data that is inaccurate.
- Where data has been processed in breach of the Act an individual may claim compensation from the data controller. It is necessary for an individual to show that they have suffered damage or damage and distress.
- Also, the data controller must be unable to prove that they had taken reasonable care in all the circumstances to comply with the Act.

**Offences**

The Act creates a number of criminal offences in relation to the processing of data. Proceedings for criminal offences can be brought by the Information Commissioner and/or the Director of Public Prosecutions. Examples of criminal offences include processing data without notification, failure to notify the Commissioner of changes to the register, failure to comply with a written request for particulars and unlawful selling of personal data. The Information Commissioner also has the power to issue enforcement notices. These may require the data controller to rectify, block, erase or destroy the data. Failure to comply with such notices is also a criminal offence

**Practical steps for complying with the act**

Businesses must ensure that appropriate notification is sent to the Information Commissioner. A person should be appointed in the business to oversee compliance with the Act. They should be responsible for overseeing things such as:

- Ensuring that all data capture forms comply with the Act and that data is obtained fairly. For example informing the individual why the data is required and what the organisation will use it for.
- Providing data subjects with an opportunity to check and update personal data held in relation to them.
- Ensuring that the data is adequately secure. For example, filing cabinets can be locked and that computer systems are secure.
- Making sure that access to data requests are dealt with correctly.
- The manner of collecting information on employees and others at all stages of the employment process.
- Where records are held over a period of time those records are reviewed regularly to ensure that unnecessary data is deleted and existing data updated.

- How long disciplinary records are kept.
- What type of sensitive personal data is held and for what purposes.
- The arrangements in place for reviewing the details notified to the Commissioner.

**Codes of Practice**

The Information Commissioner's Office has produced a number of codes of practice and guidance documents to ensure that data processing in certain areas is carried out in accordance with the Act. The following are examples of guides available:

- The Employment Practices Code
- Code of Practice on Telecommunications Directory Information and Fair Processing.
- Getting it right: a brief guide to data protection for small businesses
- Health data: use and disclosure
- Health records: subject access
- Model contracts for transfer to other organisations
- Checklist for handling requests for personal information (subject access requests)

**Exemptions**

There are a number of total exemptions and modifications to the Act. These are contained in Sections 28-36, Schedule 7 and instruments made under the Act. Further advice should be sought on the application of these provisions.

**Further Information**

The Data Protection Act 1998 and all related regulations are freely available at www.statutelaw.gov.uk.

The Information Commissioner's Office website contains extensive guidance on the Act. www.ico.gov.uk.

Alternatively the Information Commissioner can be contacted at:

The Information Commisioner's Office,
Wycliffe House, Water Lane,
Wilmslow, Cheshire, SK9 5AF

Helpline: 08456 306060 or 01625 545745 Fax: 01625 524510