GDPR - DATA PROTECTION POLICY

STATEMENT OF INTENT

Next Level Sports Ltd (NLS) is fully committed to comply with the requirements of the Data Protection Act 1998 ("the Act"). NLS will therefore follow procedures that aim to ensure that all employees are fully aware of and abide by their duties and responsibilities under the Act. We will comply with the latest GDPR data protection laws.

AIMS

In order to operate efficiently, NLS has to collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, clients, customers and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government and to share information when requested. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Act to ensure this.

NLS regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence NLS and those with whom it carries out business NLS will ensure that it treats personal information lawfully and correctly.

METHODS

The Act stipulates that anyone processing personal data must comply with Seven Principles of good practice.

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.
- Personal data shall be 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.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- 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.

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

The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and "sensitive" personal data.

Personal data is defined as, data relating to a living individual who can be identified from:
That data;

- That data and other information which is in the possession of or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Criminal proceedings or convictions.

HANDLING OF PERSONAL/SENSITIVE INFORMATION

NLS will, through appropriate management and the use of strict criteria and controls: -

- Observe fully conditions regarding the fair collection and use of personal information;
- Meet its legal obligations to specify the purpose for which information is used;
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Apply strict checks to determine the length of time information is held;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards;
- Ensure that the rights of people about whom the information is held can be fully exercised under the Act.
- All data is stored in a locked cabinet.

These include:

- The right to be informed that processing is being undertaken;
- The right of access to one's personal information within the statutory 30 days;
- The right to prevent processing in certain circumstances;
- The right to correct, rectify, block or erase information regarded as wrong information.

All managers and staff of NLS will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically;
- Individual passwords should be such that they are not easily compromised.
- All data is stored in a locked cabinet.

DATA PROTECTION OFFICER

Luke and Scott are the nominated officers on the Data Protection Register.

Key Responsibilities:

- Develop and implement the organisation's Data Protection Policy.
- Create 'best practice' guidance for data processors, preferably in written form for future reference.
- Train and advise staff on the provisions of the Data Protection Act.
- Identify and monitor the data processors whilst at work, ensuring that they deal with data in a manner consistent with the 8 data protection principles.
- Process and respond to all requests for information by data subjects.
- Ensure data remains up-to-date and is destroyed when necessary.
- Audit of all personal data, this is not just customers or parents or children but also staff.
- Understand where the data is coming from and most importantly who it is shared with.
- Set clear processes of how we handle to data for staff to work to

- Review of Terms and Conditions, Privacy and Consent notices, Website, Cookie notices.
- Ensure third parties who hold our data are fully compliant to GDPR regulations
- Is the person responsible for investigating and reporting personal data breaches
- Ensures the correct procedures are in place to detect, report and investigate a personal data breach.
- Ensures the organisation is registered with the ICO.

NOTIFICATION TO THE INFORMATION COMMISSIONER'S OFFICE

The Information Commissioner maintains a public register of data controllers and NLS is entered on this register.
The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.

The registered data controller for NLS is: Scott and Luke the directors, and they are responsible for notifying and updating the Information Commissioner's Office.

The register entry for NLS contains personal data held for 6 purposes.

1. Staff Administration
2. Advertising, Marketing and Public Relations
3. Accounts & Records
4. Provision of Child Care
5. Education
6. Crime Prevention & Prosecution of Offenders

BREACHES OF THE CODE (INCLUDING BREACHES IN SECURITY)

Any breach of this policy by NLS staff will be initially investigated by Luke or Scott, the registered controller in order, for them to take appropriate disciplinary action.

Any serious breach of the Code of Practice will be investigated immediately, and recommendations made on how to prevent any repetition of the breach. This will be reported to the ICO within 72 hours.

COMPLAINTS

Any complaints about the recording and storage of data should be made in writing, and addressed to Scott or Luke (Directors).

All complaints will be investigated in accordance with this policy.

Storage, retention and destruction of child protection records.

All information about child protection concerns are kept separate from the child's general record in individual files in a secure and locked cabinet. The child protection records are passed into the child's new setting or school and are kept until they are 25. When the retention period finishes the confidential records will then be shredded and all electronic versions are purged.

Storage, retention and destruction of concerns about adult's behaviour.

All information about concerns of adult's behaviour are kept in the person's confidential file. The concerns are kept in the person's individual file for 10 years or until the person reached 65 whichever is longer. The records are kept for the same amount of time regardless of whether the allegations were unfounded. Any concerns that are found to be malicious are destroyed immediately.