



Data Protection Policy – TNT Fitness

Policy information	
Organisation	TNT Fitness are responsible for the collection of personal data for computerised bookings, memberships and emails in relation to TNT Fitness events, products and services only. TNT Fitness's appointed data controller is: Taylor Scaife.
Scope of policy	<p>This policy applies to TNT Fitness Guisborough and Whitby and is applicable to all personal data in any format visual, written, electronic or otherwise.</p> <p>Data Processors acting on your behalf of TNT Fitness:</p> <p>GoCardless (Direct debits). https://gocardless.com/</p> <p>Mailchimp (Email services). https://mailchimp.com/</p> <p>Worldpay (Card processing). https://business.worldpay.com</p> <p>iPage (Web hosting). https://www.ipage.com/</p>
Policy operational date	25 th May 2018
Policy prepared by	Taylor Scaife (Data Protection Officer).
Date approved by Board/ Management Committee	Approved by TNT Fitness Managing Directors: Taylor Scaife & Edward James Turner on the 21 st May 2018
Policy review date	25 th May 2021

Introduction	
Purpose of policy	<ul style="list-style-type: none"> • Compliance with GDPR legislation • Protection of clients, staff and other individuals data • Protection the organisation • To maintain good practice
Types of data	<p>Data processed by TNT Fitness:</p> <p>Personal (Non sensitive data)</p> <ul style="list-style-type: none"> › Full name › Gender › Address › Contact number › Emergency contact details › Relevant medical conditions › Email address (Only when opted in) › Membership / Booking type › Purchases / membership package
Policy statement	<ul style="list-style-type: none"> › To let customers, partners, organisations and individuals clearly and transparently know how their data is used, stored, protected and processed by TNT Fitness in a clear way. › To comply with both the law and good practice › To respect individuals' rights regarding their data. › To be open and honest with individuals whose data is held / processed. › To provide training and support for staff who handle personal data, so that they can act confidently and consistently. › Notify the Information Commissioner voluntarily, even if this is not required when and where appropriate to better the service we offer and protect individuals rights. <p>Please also note the information on individuals' rights which is can be found here: (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/)</p>
Key risks	<ul style="list-style-type: none"> › Local data being stolen or destroyed. › Inappropriate disclosure of information. › Unauthorised access of computer systems. › Inaccurate information being held. › 3rd Party data processing services being compromised.

Responsibilities	
Company Directors	Have overall responsibility for ensuring that the organisation complies with its legal obligations.
Data Protection Officer	<p>TNT Fitness company director: Taylor Scaife.</p> <p>Their responsibilities include:</p> <ul style="list-style-type: none"> • Briefing the Board/ partners on Data Protection responsibilities • Reviewing Data Protection and related policies • Advising other staff on tricky Data Protection issues • Ensuring that Data Protection induction and training takes place • Notification to the ICO • Handling subject access requests • Approving unusual or controversial disclosures of personal data • Approving contracts with Data Processors
Specific Department Heads	Company directors: Taylor Scaife and Edward J Turner working alongside any other managers appointed.
Employees & Volunteers	All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work. (From now on, where 'employees' is used, this includes both paid employees and volunteers.)
Enforcement	Penalties for infringing Data Protection and related policies. Include: Immediate dismissal with loss of holiday pay, written warning or suspension from work. All infringements are recorded and actioned. One to one training is given to all staff and recorded, standards are monitored and support is offered to every member of staff.

Security	
Scope	To ensure that data security measures are in place to appropriately protect all personal and company data.
Setting security levels	Security / Confidentiality levels are set as follows 1: Booking information / class registers (Low) 2: Personal details (Med/High) 3: Bank details or information of a sensitive or strict confidential manner.
Security measures	For each confidentiality / Security level the following security measures are in place: Level 1: Information is available to all members of staff either printed / written or password protected through our gm bookings system. Level 2: Client typically fills out details on TNT Par Q form (TNT-PSCF2-001/2) Member of staff securely stores this and returns to TNT HQ, information is then entered into gym bookings system and then secured in a locked filing cabinet. All information is stored locally and double password protected information at this level follows a clear desk policy. Level 3: We currently do not hold or process any bank details or deal with any information classed as level 3. All computer systems are password protected with auto-lock functions and staff are asked to follow a clear desk policy as good practice.
Business continuity	All gym bookings systems are backed up and encrypted weekly to enable system restoration and business continuity in the event of theft or fire.
Specific risks	No personal details are to be taken home by any member of staff other than registers or newly filled out TNT Par Q forms (TNT-PSCF2-001/2) by members of staff who are unable to return to TNT HQ before close of business, in these special circumstances all details must be treated with utmost confidentiality, stored securely and returned to TNT Fitness HQ for processing as soon as practically possible. No members of staff are allowed to access or action any personal or company data without prior authorisation other than as part of their day to day job role. Staff are trained and educated in 'Scams' such as "vishing" and "phishing" where employees are tricked into giving away information over the phone or by email. No details are to be given via any method without express authorisation from either company director.

Data recording and storage	
Accuracy	Accuracy of information is important to us and all clients / customers are asked to fill out TNT Par Q forms (TNT-PSCF2-001/2) even if basic details have already been entered previously when for example making a telephone booking. Details are checked as they are entered onto our bookings system and any discrepancies rectified after confirmation with client / customer.
Updating	<p>Digital booking / GymMaster customer / client information is checked on a yearly basis alongside our financial year end, any data no longer active is automatically marked by the system as 'expired' following the retention periods set out below all data is then removed and destroyed in both digital and hard copy once it reaches the set retention period.</p> <p>Information is also checked on the system at the same time as our financial year end and updated if required.</p> <p>CVs for more than 6 months unless you have express permission from the candidates</p>
Storage	All information is stored either in locked filing cabinets (Hard copy) or double password protected on TNT HQ Booking PC (Digital). Encrypted digital system backups are also cloud stored weekly on our data server to enable data restoration in the event of theft or fire.
Retention periods	<p>Accident Records: 6 years since the last entry, or if it involves a child until they reach 21 + 6 Years.</p> <p>Income Tax and NI: 3 years from the end of the financial year to which they relate.</p> <p>Maternity and Paternity: 3 years from the end of the tax year in which the leave ends.</p> <p>Salary and Pay: 6 years.</p> <p>Working Time: 2 years.</p> <p>Application and Recruitment Records: 6-12 months.</p> <p>Parental Leave: 5 years from birth or adoption, or 18 years if the child receives a disability allowance.</p> <p>Pension Benefits: 12 years from the ending of any benefit payable.</p> <p>All Personnel Files / Client and Training Records: 6 years from the end of employment.</p> <p>Redundancy Records: 6 years.</p> <p>Sickness Absence Records: 6 years after employment ends.</p> <p>Client Records: Adults 6 Years after last charge to account / booking or transaction. Child as above but records are kept until child reaches the age of 21 + 6 Years from that date.</p> <p>GDPR Data Access Requests: 6 Years from date of request.</p>

Archiving	<p>All non active data still required to be stored / archived will be stored in a secure manner either digitally encrypted / Double password protected. Hard copies of data will be locked away in secure filing cabinets or stored in storage boxes behind a locked door.</p> <p>Data due to be destroyed (post retention data) will be erased from all systems and backups. Hard copies will be cross shredded or incinerated and all data will be made irrecoverable.</p>
------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Right of Access	
Responsibility	Taylor Scaife as Data Protection Officer is responsible for processing 'Right of access' requests. All requests are to be handled within the legal time limit which is one month from receipt of the written request.
Procedure for making request	Right of access requests must be in writing using form TNT-DATA-ROAR-01 available on request via phone, email or in person. All TNT employees have a responsibility to pass on anything which might be a subject access request to the appropriate person without delay.
Provision for verifying identity	Where the person managing the access procedure does not know the individual personally or there is any question of an individual's identity, verification of the individual seeking 'Right of Access' should be clarified before handing over any information. Verification should be made by checking 2 x identity documents one of which must be either, photo card driving license, passport or birth certificate. The second could be a utility bill, payslip, or government communication. All must be valid and in date, letters or bills must be no older than 6 months old.
Charging	Requests for data are free of charge provided it is a first request form received within a 12 month period if there are multiple requests for information within the same 12 months the TNT Fitness reserve the right to charge a reasonable fee of £10.00 per request to cover admin cost / time and printing charges this also applies to multiple copies of the same report / request of data.
Procedure for granting access	<p>If the request is made electronically, identity must be verified before any information can be disclosed.</p> <p>Information is available in PDF (Digital) and printed (Hard copy) from depending on which has been requested.</p> <p>As TNT Fitness do not have or offer any online services and our system and data are stand-alone we are unable to offer any automated request for information or an autonomous service at this time.</p>

Transparency	
Commitment	<p>TNT Fitness are committed to ensuring that you know why we hold your data, for how long and how we use that data. If that isn't already clear from earlier sections in this policy we have bullet pointed the key reasons below to help you better understand:</p> <ul style="list-style-type: none"> • Your data is processed / stored for booking and purchases in relation to attendances / memberships and products at TNT Fitness. • With your consent we use your email address to keep in touch and provide you with TNT offers and information on events. • We never store or collect your bank details as we have a 3rd party (GoCardless) who take care of that for us. • We never disclose any of your personal details unless it is a matter of safety / life or death or with your consent • You can request access to the data we hold or offer any changes to it at any time.
Procedure	<p>Information on how we store and process data and responsibilities and rights are covered in:</p> <ul style="list-style-type: none"> • Staff training • In this policy • TNT Par Q forms (TNT-PSCF2-001/2) • On our web site
Responsibility	<p>As we are a small organisation responsibility comes down to the two managing directors: Taylor Scaife and Edward James Turner both of whom work closely with all members of staff on a daily basis.</p>

Lawful Basis	
Underlying principles	<p>GDPR states you must record the lawful basis for the personal data you hold, these are the reasons we hold and process such data:</p> <p>Consent: We have consent from individuals to process their data as specified in this policy for booking ect.</p> <p>Legal Obligation: We have to maintain accident record, staff sickness and other records of a legal nature.</p> <p>Vital Interests: Certain information is vital to protect life or reduce risk of injury.</p>
Opting out	You are able to opt out of any email marketing or such like at any time by following the 'opt-out' or 'Unsubscribe links at the bottom or any of communications or by contacting a member of staff.
Withdrawing consent	You may withdraw consent at any time however this cannot be retrospectively. Data may be retained where legally required or if client or member still owes money to TNT Fitness limited. Any data retained will be retained in line with this policy.

Employee training & Acceptance of responsibilities	
Induction	All employees who have access to any kind of personal data have their responsibilities outlined during their induction. Employees are updated / trained when changes in data policy, laws or procedure take place.
Continuing training	Data protection is to be considered on a regular matter in staff and management meetings giving opportunities to better improve our security and services and deal with any flaws or faults in our systems regarding data protection.
Procedure for staff signifying acceptance of policy	All staff are given a copy of all TNT Fitness policies and key areas highlighted and raised in training and when working one to one with staff. Staff training covers certain areas and major policy changes to better aid staff in their job, keep our standards high and enable understanding with regards to their responsibilities. Employees also sign and agree to all of our policies when signing their terms of employment.

Policy review	
Responsibility	Taylor Scaife (Data Protection Officer).
Procedure	<p>Consultation will take place with both owners of the business, partners and 3rd party organisations (if applicable) and key members of staff. Information will be gathered from government sources such as:</p> <p>https://ico.org.uk/ (Information Commissioners office).</p> <p>https://www.gov.uk/ (Government website UK).</p> <p>https://www.eugdpr.org/ (EU General Data Protection Regulation website)</p>
Timing	<p>Review period to be started 25th March 2021 in order to meet the deadline of: 25th May 2021</p> <p>NOTE: Review may take place earlier if either:</p> <ul style="list-style-type: none"> • Major faults or ongoing issues are raised with this policy. <p>or</p> <ul style="list-style-type: none"> • The law changes effecting guidelines or legal requirements within this policy.

END