National Association of Tangent Clubs
Data Protection Policy

CONTENTS

Data Protection Policy

1 Overview

National Association of Tangent Clubs (”NATC”) takes the security and privacy of personal information seriously. As part of our activities we need to gather and use personal information about a variety of people including members, former members, Executive Officers and generally people who are in contact with us. The Data Protection Act 2018 (the “2018 Act”) and the EU General Data Protection Regulation (“GDPR”) regulate the way in which personal information about living individuals is collected, processed, stored or transferred.

This policy explains the provisions that we will follow when any personal data belonging to or provided by data subjects, is collected, processed, stored or transferred on behalf of NATC. We expect everyone processing personal data on behalf of NATC (see paragraph 5 for a definition of “processing”) to comply with this policy in all respects.

NATC has a separate Privacy Notice (“Personal information under the General Data Protection Regulation”) which outlines the way in which we use personal information provided to us. A copy can be obtained from the website or from the National Secretary

All personal data will be held in accordance with the NATC’s Data Retention Policy, which must be read alongside this policy. A copy of the Data Retention Policy can be obtained from the National Secretary. Data should only be held for as long as necessary for the purposes for which it is collected.

It is intended that this policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, NATC intends to comply with the 2018 Act and the GDPR.

All National Executive Officers will comply with this Policy

2 Data Protection Principles

Personal data will be processed in accordance with the six ‘**Data Protection Principles**.’ It must be:

- processed fairly, lawfully and transparently;

- collected and processed only for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- accurate and where necessary kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

NATC and its Executive Officers are accountable for these principles and must be able to demonstrate compliance.

3 Definition of personal data

3.1 **"Personal data"** means information which relates to a living person (a "data subject") who can be identified from that data on its own, or when taken together with other information which is likely to come into the possession of the data controller. It includes any expression of opinion about the person and an indication of the intentions of the data controller or others, in respect of that person. It does not include anonymised data.

3.2 This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

4 Special categories of personal data

4.1 NATC does not and will not hold any special categories of personal data

5 Definition of processing

5.1 **'Processing'** means any operation which is performed on personal data, such as collection, recording, organisation, structuring or storage; adaption or alteration; retrieval, consultation or use; disclosure by transmission, dissemination or otherwise making available; and restriction, destruction or erasure.

6 How personal data should be processed

6.1 Everyone who processes data on behalf of NATC has responsibility for ensuring that the data they collect and store is handled appropriately, in line with this policy, our Data Retention policy and our Privacy Notice.

6.2 Personal data should only be accessed by those who need it for the tasks they do for or on behalf of NATC. Data should be used only for the specified lawful purpose for which it was obtained.

6.3 The legal basis for processing personal data is that the processing is necessary for the purposes of NATC's legitimate interests;

6.4 Personal data held in all manual and digital files and the contact spreadsheet should be kept up to date. It should be shredded or disposed of securely when it is no longer needed. Unnecessary copies of personal data should not be made.

7. Privacy Notice

7.1 In relation to its Forms NATC will issue the Privacy Notice ("Personal information under the General Data Protection Regulation") at the point when data is provided.

7.2 NATC will make the Privacy Notice ("Personal information under the General Data Protection Regulation") available on its website

7.3 NATC will make the Privacy Notice ("Personal information under the General Data Protection Regulation") available on request from its National Secretary

8. Keeping personal data secure

8.1 Personal data should not be shared with those who are not authorised to receive it. Care should be taken when dealing with any request for personal information such as email addresses.

8.2 Hard copy personal information should be stored securely (in lockable storage, where appropriate) and not visible when not in use. Filing cabinets and drawers and/or office doors should be locked when not in use. Keys should not be left in the lock of the filing cabinets/lockable storage.

8.3 Digital copy personal information should be stored securely on Password Protected /Encrypted devices.

8.4 Passwords should be kept secure, should be strong, changed regularly and not written down or shared with others.

8.5 Emails containing personal information should not be sent to or received at a work email address as this might be accessed by third parties.

8.6 The 'bcc' rather than the 'cc' or 'to' fields should be used when emailing more than one person;

8.7 If personal devices have an @tangent-clubs.org account linked to them these should not be accessed on a shared device for which someone else has the pin code.

8.8 Personal data should be encrypted or password-protected before being transferred electronically. All NATC @@tangent-clubs.org accounts will be encrypted.

8.9 Personal data should never be transferred outside the European Economic Area except in compliance with the law. This is particularly relevant to communications with Tangent Club International.

9. Sharing personal data

9.1 NATC will only share someone's personal data where the Association has a legal basis to do so.

9.2 NATC will not send any personal data outside the European Economic Area. If this changes all individuals affected will be notified and the protections put in place to secure their personal data, in line with the requirements of the GDPR;

10. How to deal with data security breaches

10.1 Should a data security breach occur, the National Secretary will be advised **immediately.** If the breach is likely to result in a risk to the rights and freedoms of individuals then the Information Commissioner's Office must be notified within 72 hours.

11. Subject access requests

11.1 Data subjects can make a subject access request to find out what information is held about them. This request must be made in writing. Any such request received by the

Association or any Executive Officer should be forwarded immediately to the National Secretary who will coordinate a response within the 30 days time limit.

11.2 It is a criminal offence to conceal or destroy personal data which is part of a subject access request.

12. Data subject rights

12.1 Data subjects have certain other rights under the GDPR. This includes the right to know what personal data NATC processes, how it does so and the legal basis for doing so.

12.2 Data subjects also have the right to request that NATC corrects any inaccuracies in their personal data, and erase their personal data where NATC is not entitled by law to process it or it is no longer necessary to process it for the purpose for which it was collected. Data should be erased when an individual revokes their consent (and consent is the basis for processing); when the purpose for which the data was collected is complete; or when compelled by law.

12.3 All requests to have personal data corrected or erased should be passed to the National Secretary who will be responsible for responding to them in liaison with the appropriate Executive officer.

14. Contracts

14.1 If any processing of personal data is to be outsourced to 3rd Parties, NATC will ensure that the mandatory processing provisions imposed by the GDPR will be included in the agreement or contract.

15. Policy review

The National Executive will be responsible for reviewing this policy from time to time and updating the membership and members in relation to its data protection responsibilities and any risks in relation to the processing of data.

(May 2018)