***Dartmouth & District Conservative Club***

*Privacy Policy*

This document sets out the Club’s policy on handling information about people (often referred to as personal data processing).

* **Definitions:**

|  |  |
| --- | --- |
| **Automated Decision-Making (ADM)** | when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. |
| **Automated Processing** | any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual. |
| **Club Personnel** | all employees, workers, contractors, agency workers, committee members, club members and trustees. |
| **Consent** | agreement which must be freely given, specific, informed and an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them. |
| **Data Controller** | the person or organisation that determines when, why and how to process Personal Data. We are the Data Controller of all Personal Data relating to Club Personnel and Personal Data used in the Club’s business and activities. |
| **Data Subject** | a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may have legal rights regarding their Personal Data. |
| **Data Privacy Impact Assessment (DPIA)** | tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data. |
| **Explicit Consent** | consent which requires a very clear and specific statement (that is, not just action). |
| **General Data Protection Regulation (GDPR)** | the General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the GDPR. |
| **Personal Data** | any information identifying a Data Subject or information relating to a Data Subject whom we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. |
| **Personal Data Breach** | any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach. |
| **Privacy by Design** | implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR. |
| **Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies** | separate notices setting out information that may be provided to Data Subjects when the Club collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose. |
| **Processing or Process** | any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties. |
| **Pseudonymisation or Pseudonymised** | replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure. |
| **Sensitive Personal Data** | information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions. |

* **Introduction**
* This Privacy Standard sets out how the Club handles the Personal Data of our members, suppliers, employees, workers and other third parties.
* This Privacy Standard applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, members or supplier contacts, website users or any other Data Subject.
* This Privacy Standard applies to all Club Personnel ("you", "your"). You must read, understand and comply with this Privacy Standard when Processing Personal Data on our behalf and attend training on its requirements. This Privacy Standard sets out what we expect from you in order for the Club to comply with applicable law. Your compliance with this Privacy Standard is mandatory.
* This Privacy Standard is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the Secretary.
* **Scope**
* We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the Club and will provide for successful Club operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Club is at risk of fines of up to 4% of its total annual turnover, depending on the breach, for failure to comply with the provisions of the GDPR.
* [The Committee] is responsible for ensuring all Club Personnel comply with this Privacy Standard and will implement appropriate practices, processes, controls and training to ensure such compliance.
* The Secretary is responsible for overseeing this Privacy Standard and, as applicable, developing guidelines to help with compliance.
* Please contact the Secretary with any questions about the operation of this Privacy Standard or the GDPR or if you have any concerns that this Privacy Standard is not being or has not been followed. In particular, you must always contact the Secretary in the following circumstances:
* if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests of the Club) (see paragraph 5.1UPDATE FC below);
* if you need to rely on Consent and/or need to capture Explicit Consent (see paragraph 5.2UPDATE FC below);
* if you are unsure about the retention period for the Personal Data being Processed (see paragraph 9UPDATE FC below);
* if you are unsure about what security or other measures you need to implement to protect Personal Data (see paragraph 10.1UPDATE FC below);
* if there has been a Personal Data Breach (paragraph 10.2UPDATE FC below);
* if a Data Subject invokes any of their rights (see paragraph 12UPDATE FC);
* whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see paragraph 13.5UPDATE FC below) or plan to use Personal Data for purposes other than ones for which it was collected;
* if you intend to do any direct marketing;
* if you intend to do any Automated Decision-Making or Automated Processing;
* or if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (see paragraph 13.8UPDATE FC below).
* **Personal data protection principles**
* We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:
* Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).
* Collected only for specified, explicit and legitimate purposes (Purpose Limitation).
* Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).
* Accurate and where necessary kept up to date (Accuracy).
* Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).
* Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).
* Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).
* Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).
* We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).
* **Lawfulness, fairness, transparency**
* Lawfulness and fairness:
* Personal Data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.
* You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but to ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.
* the GDPR allows Processing for specific purposes, some of which are set out below:
* the Data Subject has given his or her Consent;
* the Processing is necessary for the performance of a contract with the Data Subject;
* to meet our legal compliance obligations;
* to protect the Data Subject's vital interests;
* to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices.
* It is our policy only to collect and retain the information about people which is described in our Privacy Notices and to use it only for the purposes set out in them. You should not collect and retain any other data or use any data we hold for any other purpose. This will ensure that you have a legal ground for any Processing activity.
* Consent:
* A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.
* A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action and so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.
* Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.
* Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data, for Automated Decision-Making and for cross border data transfers. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data. Where Explicit Consent is required, you must issue a Fair Processing Notice to the Data Subject to capture Explicit Consent.
* You will need to evidence Consent captured and keep records of all Consents so that the Club can demonstrate compliance with Consent requirements.
* Transparency (notifying data subjects):
* The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices or Fair Processing Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.
* Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the GDPR including the identity of the Data Controller, how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.
* It is our policy not to collect data from third parties, other than sources open to the public. If you collect data from a third party and intend to retain it, you must notify the Secretary immediately.
* You must use the Club’s approved Privacy Notices.
* **Purpose limitation**
* Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.
* You cannot use Personal Data for new, different or incompatible purposes from those disclosed when it was first obtained, unless you have informed the Data Subject of the new purposes and they have Consented where necessary.
* **Data minimisation**
* Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.
* You may only Process Personal Data when the performance of your duties requires it. You must not Process Personal Data for any reason unrelated to your duties.
* You may only collect Personal Data that you require for your duties: do not collect more data than this. Ensure any Personal Data collected is adequate and relevant for the intended purposes.
* You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Club's data retention guidelines.
* **Accuracy**
* Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.
* You must ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.
* **Storage limitation**
* Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.
* You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it, including for the purpose of satisfying any legal, accounting or reporting requirements.
* The Club will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. You must comply with the Club's guidelines on Data Retention.
* You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Club's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.
* You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined by using the Club’s approved Privacy Notice.
* **Security integrity and confidentiality**
* Protecting Personal Data:
* Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.
* We will develop, implement and maintain safeguards appropriate to the Club’s size, and scope, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.
* You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.
* You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.
* You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:
* confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it;
* integrity means that Personal Data is accurate and suitable for the purpose for which it is processed;
* availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.
* You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data.
* Reporting a Personal Data Breach:
* the GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.
* we will put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.
* if you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the Secretary. You should preserve all evidence relating to the potential Personal Data Breach.
* **Transfer limitation**
* The GDPR restricts data transfers to countries outside the European Economic Area in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.
* You must not transfer data to anyone who is located outside the United Kingdom.
* **Data Subject's rights and requests**
* Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:
* withdraw Consent to Processing at any time;
* receive certain information about the Data Controller's Processing activities;
* request access to their Personal Data that we hold;
* prevent our use of their Personal Data for direct marketing purposes;
* ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
* restrict Processing in specific circumstances;
* challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
* prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
* be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
* make a complaint to the supervisory authority; and
* in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.
* You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).
* You must immediately forward any Data Subject request you receive to the Secretary.
* **Accountability**
* The Data Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.
* The Club must have adequate resources and controls in place to ensure and to document GDPR compliance including:
* appointing someone accountable for data privacy;
* implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;
* integrating data protection into internal documents;
* regularly training Club Personnel on the GDPR, this Privacy Standard, and any related policies and guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Club must maintain a record of training attendance by Club Personnel; and
* regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.
* Record keeping:
* the GDPR requires us to keep full and accurate records of all our data Processing activities.
* you must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.
* these records should include, at a minimum, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place.
* Training and audit:
* we are required to ensure all Club Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.
* you must undergo all mandatory data privacy related training.
* you must regularly review all the systems and processes under your control to ensure they comply with this Privacy Standard and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.
* Privacy By Design and Data Protection Impact Assessment (DPIA):
* we are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.
* you must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:
* the state of the art;
* the cost of implementation;
* the nature, scope, context and purposes of Processing; and
* the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.
* if you think a DPIA is needed, because of something you plan to do, you must tell the Secretary, who will decide what needs to be done.
* Automated Processing (including profiling) and Automated Decision-Making:
* generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:
* a Data Subject has Explicitly Consented;
* the Processing is authorised by law; or
* the Processing is necessary for the performance of or entering into a contract.
* it is our policy not to do Automated Processing (including profiling) or Automated Decision-Making and, in the unlikely event of your needing to do this, you must contact the Secretary first.
* Direct marketing:
* particular rules and privacy laws apply to unsolicited direct marketing.
* for example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls).
* the right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.
* a Data Subject's objection to direct marketing must be promptly honoured. If someone opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.
* it is our policy not to do direct marketing and, in the unlikely event of your needing to do this, you must contact the Secretary first.
* Sharing Personal Data:
* Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.
* You may only share the Personal Data we hold with another employee or volunteer, or a member of the committee if the recipient has a Club-related need to know the information.
* You may only share the Personal Data we hold with third parties, such as our service providers if:
* they have a need to know the information for the purposes of providing the contracted services;
* sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
* the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place; and
* a fully executed written contract that contains GDPR approved third party clauses has been obtained.
* **Changes to this Privacy Policy**
* We reserve the right to change this Privacy Policy at any time, so please check back regularly to obtain the latest copy of it.
* **Acknowledgement of receipt and review**

I, ................................], acknowledge that on .......................2018, I received and read a copy of the Club’s Privacy Policy, dated 25 May 2018 and understand that I am responsible for knowing and abiding by its terms. This Privacy Policy does not set terms or conditions of employment or form part of an employment contract.

Signed ……………………………………………………….

Printed Name ……………………………………………….

Date ………………………………………………………….