PRIVACY STANDARD

1. Overview

1.1 As an organisation, Norfolk County Golf Limited ("**NCG**", "**we**", "**us**, "**our**") values the personal information that is entrusted to us by our members, our staff, our volunteers, our officers and other third parties. It is extremely important to us that we uphold that trust in the way in which we handle, use, store and protect personal data.

1.2 We are committed to adopting high standards in our protection of data and in addressing privacy concerns. Not only are we putting in place appropriate technical and security measures, but also ensuring that we have privacy and the protection of data at the heart of our decision-making processes across the organisation.

1.3 We are dedicated to being open and transparent with individuals about how we use and handle their information.

1.4 It is also important to recognise the role of our officers, staff and volunteers when considering data protection compliance. With this in mind, we will ensure that we provide training to those who handle personal information as part of their job.

2. General Data Protection Regulation ("GDPR")

2.1 The GDPR will come into effect on **25 May 2018**.

2.2 The GDPR is an EU Regulation, and therefore will have direct effect in the UK, replacing the existing Data Protection Act 1998.

2.3 This Privacy Standard (and other data protection-related policies operated by NCG) have, where possible, been written with the implementation of GDPR in mind. However, please note that as the GDPR is not yet in force, these documents will need to be reviewed and updated on an ongoing basis to ensure compliance.

2.4 Fundamental to the GDPR is a new standard of accountability. All organisations, including NCG, will be required to demonstrate and evidence how they comply with the data protection principles (as set out further in this Privacy Standard). Compliance with this Privacy Standard (and our other data protection-related policies) will assist us in doing so.

3. About this Privacy Standard

3.1 This Privacy Standard applies to all staff unless otherwise indicated. The Privacy Standard therefore applies to officers, employees (whether part-time or fixed term), volunteers, consultants, contractors, agents, casual and temporary or agency staff (collectively referred to as "**Personnel**", "**you**", "**your**").

3.2 This Privacy Standard may be amended from time to time and Personnel will be directed to certain parts of the Privacy Standard as and when it is reviewed and updated.

3.3 This Privacy Standard does not form part of any employee's contract of employment or any other Personnel's contractual terms.

3.4 The officers of NCG will have overall responsibility for data protection compliance within the organisation and for ensuring this Privacy Standard (together with other data protection-related policies operated by NCG) are adhered to and comply with the relevant legal obligations.

3.5 This Privacy Standard will be reviewed from time to time by the officers to ensure that its provisions continue to meet the relevant legal obligations and reflect best practice.

3.6 We recognise that the correct and lawful treatment of personal data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. It is important to note that NCG is exposed to potential fines of up to €20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

3.7 Mike Devlin, our data compliance manager (the "**Data Compliance Manager**"), is responsible for overseeing data protection compliance, this Privacy Standard and, as applicable, developing and reviewing any data protection-related policies. Mike can be contacted on secretary@norfolkcountygolfunion.co.uk or 07922 202848.

Please contact the Data Compliance Manager 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 Data Compliance Manager in the following circumstances:

(a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by NCG) (see paragraph 7 below);

(b) if you need to rely on Consent and/or need to obtain Explicit Consent (see paragraph 7.2 below);

(c) if you need to draft Privacy Notices or Fair Processing Notices (see paragraph 7.3 below);

(d) if you are unsure about the retention period for the Personal Data being processed (see paragraph 11 below);

(e) if you are unsure about what security or other measures you need to implement to protect Personal Data (see paragraph 12.1 below);

(f) if there has been a Personal Data Breach (see paragraph 12.2 below and see also our Data Breach policy, a copy of which is available from the Data Compliance Manager);

(g) if you are unsure on what basis to transfer Personal Data outside the EEA (see paragraph 13 below);

(h) if you need any assistance dealing with any rights invoked by a Data Subject (see paragraph 14 below);

(i) whenever you are engaging in a significant new, or change in, processing activity which is likely to require a Data Protection Impact Assessment (see paragraph 15.4 below) or plan to use Personal Data for purposes others than what it was collected for;

(j) if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see paragraph 15.5 below);

(k) if you need help complying with applicable law when carrying out direct marketing activities (see paragraph 15.6 below); or

(l) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see 15.7 below).

4. Key Dates

4.1 This policy was approved by the officers of Norfolk County Golf Limited on **[*19th June 2018*]**.

4.2 This policy became operational on [25th May 2018].

4.3 This policy is next due to be reviewed [***25th May 2019***].

5. 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. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

"**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, for example to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

"**Consent**"**:** agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies 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. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Personnel and Personal Data used in our business for our own commercial purposes. NCG will be a Data Controller for most (if not all) of its business operation.

"**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.

"**Data Subjects**"**:** for the purpose of this Privacy Standard include all living individuals about whom we hold Personal Data.

"**EEA**"**:** the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

"**Explicit Consent**"**:** consent which requires a very clear and specific statement (that is, not just action).

"**Personal Data**"**:** any information identifying a Data Subject or information relating to a Data Subject that 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. For example, a member's CDH lifetime ID number would be Personal Data.

"**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)**"**:** separate notices setting out information that may be provided to Data Subjects when NCG 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.

6. Personal data protection principles

We adhere to the principles set out in the GDPR relating to the processing of Personal Data. These principles require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (*"Lawfulness, Fairness and Transparency*").

(b) Collected only for specified, explicit and legitimate purposes (*"Purpose Limitation"*).

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (*"Data Minimisation"*).

(d) Accurate and where necessary kept up to date (*"Accuracy"*).

(e) 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"*).

(f) 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"*).

(g) Not transferred to another country without appropriate safeguards being in place (*"Transfer Limitation"*).

(h) 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"*).

NCG is responsible for and must be able to demonstrate compliance with the data protection principles listed above (*"Accountability"*).

7. Lawfulness, fairness, transparency

7.1 Lawfulness and fairness

Under the GDPR, Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

We 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 ensure that we process Personal Data fairly and without unfavourably affecting the Data Subject.

The GDPR allows processing for specific purposes, some of which are set out below:

(a) the Data Subject has given his or her Consent;

(b) the processing is necessary for the performance of a contract with the Data Subject;

(c) to meet our legal compliance obligations;

(d) to protect the Data Subject's vital interests;

(e) to pursue our legitimate interests for purposes where they are not overridden because the processing harms 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 Fair Processing Notices.

In compliance with the GDPR, we must identify and document the legal ground being relied on for each processing activity (as set out in this Privacy Standard).

For specific details about the Personal Data that we process and the legal ground on which are relying to process the Personal Data, please see our processing activity register (a copy of which is available from our Data Compliance Manager).

7.2 Consent

We 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**, so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters (for example, our competition terms and conditions), then the Consent must be kept separate from those other matters. For example, we cannot refuse entry to a competition if a Data Subject does not Consent for the purposes of marketing communications.

If NCG has relied on Consent for the processing of Personal Data, Data Subjects must be easily able to withdraw Consent to processing at any time. Withdrawal must be as easy to communicate as it was initially obtained, and must be promptly honoured. Consent may need to be refreshed (i.e. new Consent obtained from the Data Subject) if you intend to process Personal Data for a different purpose, which was not disclosed when the Data Subject first gave their Consent.

Unless we can rely on another legal basis of processing, Explicit Consent is usually required for processing Sensitive Personal Data, for any Automated Decision-Making carried out by NCG and for cross border data transfers. In most cases, we will be relying on another legal basis (and not require Explicit Consent) to process most types of Sensitive Personal Data. Where Explicit Consent is required, we must issue a Fair Processing Notice to the Data Subject to obtain their Explicit Consent.

Given the nature of our organisation, we may from time to time need to undertake Disclosure and Barring Service ("**DBS**") checks on volunteers who work at volunteers or otherwise assist NCG. When doing so, we will process any Sensitive Personal Data relating to criminal convictions only where it is authorised by law (for example, where the volunteer's role involves working with vulnerable adults or children).

Save for the above paragraph, we expect that it is unlikely that Personnel will need to process Sensitive Personal Data, unless for example, we need to collect medical information or dietary requirements on juniors in relation to competitions or training.

It is very unlikely that Personnel will need to carry out Automated Decision-Making or transfer personal data across borders, given the nature of our organisation. However, if so, please contact the Data Compliance Manager before doing so to ensure that there is an appropriate legal basis on which to rely.

As an organisation, we will need to establish how and when Consent was obtained, and keep records of all Consents so that we can demonstrate compliance with Consent requirements.

7.3 Transparency (notifying Data Subjects)

The GDPR requires all Data Controllers (including NCG) 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:

(a) the purpose or purposes for which we intend to process that Personal Data, and the lawful basis of processing;

(b) the types of third parties, if any, with which we will share or to which we will disclose that Personal Data;

(c) retention period for the Personal Data or criteria used to determine the retention period;

(d) right to withdraw Consent (where appropriate);

(e) the right to complain to the Information Commissioner's Office ("**ICO**") (who are responsible for enforcing data protection in the UK); and

(f) the means, if any, by which Data Subjects can limit our use and disclosure of their Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publically available source), we must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed processing of that Personal Data.

We may use Privacy Notices or Fair Processing Notices to communicate this information to the Data Subjects, where appropriate to do so.

8. Purpose limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner that is incompatible with those purposes.

We cannot use Personal Data for any new, different or incompatible purposes from that disclosed when it was first obtained, unless we have informed the Data Subject of the new purposes and they have given Consent where necessary.

9. Data minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

We must only collect the data that we actually require to provide our services, so please do not collect excessive data beyond what is needed. We cannot process Personal Data for any reason unrelated to

the services that NCG provides. Ensure that any Personal Data collected is adequate and relevant for the intended purpose(s).

We must ensure that when Personal Data is no longer needed for specified purposes, it is deleted in accordance with our data retention register (setting out how long certain categories of Personal Data are to be stored), a copy of which is available from our Data Compliance Manager. Alternatively, the Personal Data should be anonymised so it no longer qualifies as Personal Data.

10. Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

We must ensure that the Personal Data that NCG uses and holds is accurate, complete, kept up to date and relevant to the purpose for which we collected it. Please check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You should take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data. Where possible, please ask the individual in question whether their data (for example, address, telephone number, e-mail address) is correct and up-to-date.

11. 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.

We 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.

We will maintain retention policies, registers 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. Please see our data retention register (setting out how long certain categories of Personal Data are to be stored), a copy of which is available from our Data Compliance Manager.

Please take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with our retention register and any relevant policies. This includes requiring third parties to delete such data where applicable.

Where necessary, we will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice or Fair Processing Notice.

12. Security integrity and confidentiality

12.1 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 our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks. We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of Personal Data. We are responsible for protecting the Personal Data that

we hold, and all Personnel must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

Please 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. Personal Data may only be transferred 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. If you have any concerns about the security of Personal Data transferred to third-party providers, please contact the Data Compliance Manager immediately.

We will maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) "**Confidentiality**" means that only people who have a need to know and are authorised to use the Personal Data can access it.

(b) "**Integrity**" means that Personal Data is accurate and suitable for the purpose for which it is processed.

(c) "**Availability**" means that authorised users are able to access the Personal Data when they need it for authorised purposes.

In order to do so, we have in place security procedures such as:

(d) **Access controls.** Only Personnel who need to access to the Personal Data will be permitted to have access.

(e) **Secure lockable storage.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

(f) **Pseudonymisation and encryption.** Encryption of files, devices and equipment to ensure that, if such files or equipment are accessed by any person who is not authorised, the data is unintelligible. Where possible, we will take steps to render Personal Data anonymous so that the Data Subject is no longer identifiable.

(g) **Methods of disposal.** Paper documents should be shredded in confidential waste. Digital storage devices should be physically destroyed when they are no longer required.

(h) **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

For details on the procedure in the event of a Personal Data Breach, please see paragraph 12.2 below and our Data Breach policy (which is available from our Data Compliance Manager).

Personnel 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.

12.2 Reporting a Personal Data Breach

The GDPR requires us to notify any Personal Data Breach to the ICO and, in certain instances, the Data Subject.

We have 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, please do not attempt to investigate the matter yourself. Immediately contact the Data Compliance Manager and follow the Data Breach policy (a copy of which is available from our Compliance Manager). You should preserve all evidence relating to the potential Personal Data Breach.

13. Transfer limitation

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You will be transferring Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

You may only transfer Personal Data outside the EEA if one of the following conditions applies:

(a) the EU has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects;

(b) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

(c) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

We do not expect that you will need to transfer Personal Data outside the EEA in the normal course of business, but if you do, please contact the Data Compliance Manager before doing so.

14. Data Subject's rights and requests

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to processing at any time;

(b) receive certain information about the Data Controller's processing activities;

(c) request access to their Personal Data that we hold;

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) 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;

(f) restrict processing in specific circumstances;

(g) challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;

(i) object to decisions based solely on Automated Processing, including profiling (ADM);

(j) prevent processing that is likely to cause damage or distress to the Data Subject or anyone else;

(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(l) make a complaint to the supervisory authority (i.e. the ICO); and

(m) 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 (and 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 Data Compliance Manager, whose details are at paragraph 3.7 above.

15. Accountability

15.1 We will implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. We are responsible for, and must be able to demonstrate, compliance with the data protection principles.

NCG has adequate resources and controls in place to ensure and to document GDPR compliance including:

(a) appointing a Data Compliance Manager as being responsible for all data protection compliance;

(b) implementing Privacy by Design when processing Personal Data and completing DPIAs where processing presents a high risk to rights and freedoms of Data Subjects;

(c) integrating data protection into internal documents including this Privacy Standard, Privacy Notices or Fair Processing Notices and other data protection-related policies;

(d) training Personnel on the GDPR, this Privacy Standard, data protection-related policies and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. We will maintain a record of training attendance by Personnel; and

(e) testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

15.2 Record keeping

The GDPR requires us to keep full and accurate records of all our data processing activities.

We 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, the name and contact details of the Data Controller (where applicable), clear descriptions of the Personal Data types, Data Subject types, processing activities, processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

15.3 Training and audit

We are required to ensure all 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 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.

15.4 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 in an effective manner, to ensure compliance with data privacy principles.

You should assess what Privacy by Design measures can be implemented on all programs/systems/processes that process Personal Data by taking into account the following:

(a) available technology;

(b) the cost of implementation;

(c) the nature, scope, context and purposes of processing; and

(d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the processing.

Data Controllers must also conduct DPIAs in relation to high risk processing.

There may be circumstances where you should conduct a DPIA (or discuss the prospect about doing so with the Data Compliance Manager) when implementing major system or business change programs involving the processing of Personal Data including:

(e) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

(f) Automated Processing including profiling and ADM;

(g) large scale processing of Sensitive Data; and

(h) large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

(i) a description of the processing, its purposes and the Data Controller's legitimate interests if appropriate;

(j) an assessment of the necessity and proportionality of the processing in relation to its purpose;

(k) an assessment of the risk to individuals; and

(l) the risk mitigation measures in place and demonstration of compliance.

15.5 Automated Processing (including profiling) and Automated Decision-Making

Generally, Automated Decision-Making is prohibited when a decision has a legal or similar significant effect on an individual unless:

(a) a Data Subject has Explicitly Consented;

(b) the processing is authorised by law; or

(c) the processing is necessary for the performance of or entering into a contract.

If certain types of Sensitive Personal Data are being processed, then grounds (b) or (c) will not be allowed but such Sensitive Personal Data can be processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

We do not expect that there will any requirement within our organisation to carry out Automated Decision-Making and only limited Automated Processing. If you are intending to carry out processing that would involve Automated Decision-Making, please contact the Data Compliance Manager before doing so.

A DPIA must also be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

15.6 Direct marketing

We are subject to certain rules and privacy laws when marketing to our members or other third parties.

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 an individual 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.

15.7 Sharing Personal Data

Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and arrangements have been put in place.

You may only share the Personal Data we hold with third parties, such as our service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) 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;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross border transfer restrictions; and

(e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

16. Changes to this Privacy Standard

We reserve the right to change this Privacy Standard at any time so please check back regularly to obtain the latest copy of this Privacy Standard. Where appropriate, we will notify you of the changes to this Privacy Standard as soon as possible.