PRIVACY STANDARD

1. INTRODUCTION

1.1 Movement for Another Future Limited ("**we**", "**our**", "**us**", or "**Office**") is the official campaign for Keir Starmer for Leader (the "**Campaign**") of the Labour Party (the "**Party**").

1.2 This privacy standard policy (the "**Privacy Standard**") sets out how the Office handles Personal Data in respect of the Campaign.

1.3 This Privacy Standard applies to you and all other members of the Campaign's office personnel ("**you**"). You must read, understand and comply with this Privacy Standard when Processing Personal Data on the Campaign's behalf. This Privacy Standard sets out what we expect from you in order to ensure that you, the Office and the Campaign comply with applicable law. Your compliance with this Privacy Standard is a mandatory condition of your involvement with the Campaign.

1.4 This Privacy Standard is an internal document and must not be shared with third parties, without prior authorisation from the Office. If you have any questions on the subject matter or content of this Privacy Standard, please contact dataprotection@keirstarmer.com ("**Head of Data Protection**").

1.5 You can locate the defined terms contained in this Privacy Standard at Annex A.

2. PERSONAL DATA PROTECTION PRINCIPLES

2.1 We adhere to the principles relating to Processing of Personal Data set out in the GDPR which 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); and

(h) made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

2.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

3. LAWFULNESS AND FAIRNESS

3.1 Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

3.2 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 ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

3.3 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 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

(f) to perform a specific task in the public interest that is set out in law.

3.4 You must identify and document the legal ground being relied on for each Processing activity.

4. CONSENT

4.1 A 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.

4.2 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, then the Consent must be kept separate from those other matters.

4.3 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.

4.4 When processing Special Category Data or Criminal Convictions Data, we will usually rely on a legal basis for processing other than explicit Consent or Consent if possible. Where explicit Consent is relied on, you must issue a Privacy Notice to the Data Subject to capture explicit Consent.

4.5 You will need to evidence Consent captured and keep records of all Consents so that the Office can demonstrate compliance with Consent requirements.

5. TRANSPARENCY

5.1 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. The information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

5.2 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 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.

5.3 When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting or 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.

5.4 If you are collecting Personal Data from Data Subjects, directly or indirectly, then you must provide Data Subjects with a Privacy Notice. If you cannot locate our Privacy Notice, or consider that there is a valid reason for the Privacy Notice not to be provided, then please contact our Head of Data Protection.

6. PURPOSE LIMITATION

6.1 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.

6.2 You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

7. DATA MINIMISATION

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

7.2 You may only Process Personal Data when performing your job duties requires it. You must not Process Personal Data for any reason unrelated to your job duties. Under no circumstances may you remove or copy Personal Data from the Office or the Campaign for any purpose unconnected to the Campaign.

7.3 You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

7.4 You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Office's data retention instructions or guidelines. Per Paragraph 9 of this Privacy Standard, all Personal Data will be reviewed at the conclusion of the Campaign, where the majority of it will be destroyed – however, if you consider that any Personal Data held by the Campaign needs to be deleted earlier, please contact the Head of Data Protection.

8. ACCURACY

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

8.2 You will 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.

9. STORAGE LIMITATION

9.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

9.2 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.

9.3 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 Office's instructions or applicable policies. This includes requiring third parties to delete that data where applicable.

9.4 The Office shall securely destroy or erase all Personal Data it receives in accordance with the rules of the Party’s National Executive Committee or any other rules which apply to the Campaign.

9.5 The Office shall on completion of the Campaign, review its purposes for Processing Personal Data and take any necessary measures required to comply with its

obligations under Data Protection Legislation, including considering whether such Personal Data should be securely destroyed or erased.

9.6 The Office shall securely destroy or erase all Personal Data it holds on, or during the process of, its dissolution – it will only retain Personal Data where it is obliged to do so by law, or where the relevant Data Subjects are aware that their Personal Data may be retained beyond the conclusion of the Campaign.

10. PROTECTING PERSONAL DATA

10.1 Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

10.2 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 (including use of encryption). 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 Special Categories of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

10.3 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.

10.4 You must 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; and

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

10.5 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.

11. REPORTING A PERSONAL DATA BREACH

11.1 Where a Personal Data Breach is identified, it must be reported to the Office immediately. A Personal Data Breach is any occasion on which Personal Data is lost, or where Personal Data is accessed or taken by a third party without the Office's knowledge and authorisation.

11.2 We set out below some of the most common examples of a Personal Data Breach so that you can more easily identify common breaches should they occur:

(a) human error where Personal Data is accidentally sent to someone (either internally or externally) who does not have a legitimate need to see it;

(b) databases containing Personal Data being compromised, for example being illegally accessed by unauthorised individuals;

(c) loss or theft of laptops, tablet devices, mobile devices, USB sticks or paper records containing personal data;

(d) paper records containing Personal Data being left unprotected for anyone to see, for example:

(i) files left out when the owner is away from their desk and at the end of the day;

(ii) papers not properly disposed of in secure disposal bins that can then be extracted or seen by others; or

(iii) papers left at photocopying machines;

(e) unauthorised disclosure of Personal Data

(f) being deceived by a third party into improperly releasing your Personal Data (or another person's Personal Data);

(g) system failure;

(h) a hacking attack; and

(i) the loss of Personal Data due to unforeseen circumstances such as a fire or flood.

11.3 All Personal Data Breaches must be reported to the Head of Data Protection in writing within 24 hours of identifying that breach. If you believe the Personal Data Breach is serious and includes, for example, any Special Categories of Personal Data or large amounts of Personal Data, the Personal Data Breach must be reported immediately.

11.4 Once reported, you will provide all requested assistance to the Head of Data Protection in recording the Personal Data Breach.

11.5 You will also provide to the Head of Data Protection any necessary information he needs so that he can assess whether the Personal Data Breach should be reported to our Supervisory Authority, the Information Commissioner, and the affected Data Subjects.

11.6 Our immediate priority will be to contain or otherwise limit the impact of the Personal Data Breach once identified. You will assist the Head of Data Protection in doing so, for example, where a Personal Data Breach occurs because you accidentally sent files containing Personal Data to an unauthorised individual, under the instruction of the Head of Data Protection, you will contact that individual asking them not to pass on that Personal Data to any third parties and to delete it immediately.

12. TRANSFER LIMITATION

12.1 The GDPR restricts data transfers to countries outside the EEA 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.

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

(a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;

(b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the Head of Data Protection;

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

(d) 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.

12.3 It is unlikely that the Campaign will need to transfer any Personal Data outside of the EEA. If you consider that such a transfer is necessary, you must speak with the Head of Data Protection for authorisation before that transfer takes place.

13. DATA SUBJECT'S RIGHTS

13.1 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;

(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; 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.

13.2 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).

13.3 You must immediately forward any Data Subject request you receive to your Head of Data Protection and comply with our Subject Access Request policy.

13.4 Do not offer any information or Personal Data to the Data Subject or agree to comply with the Data Subject without appropriate authorisation from the Head of Data Protection.

13.5 Where you are notified by a Data Subject that it would like to exercise any of its rights under Data Protection Legislation (as listed above), whether in writing or verbally, you shall inform the Head of Data Protection and comply with his instructions.

14. RECORD-KEEPING

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

14.2 You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

14.3 These records should include, at a minimum, the name and contact details of the Controller, 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. To create the records, data maps should be created which should include the detail set out above together with appropriate data flows.

15. TRAINING AND AUDIT

15.1 We are required to ensure all Office Personnel have undergone adequate training to enable them to comply with Data Protection Legislation. We regularly test our systems and processes to assess compliance.

15.2 You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training.

15.3 If you are a team leader or otherwise have any managerial responsibility in relation to the Processing of Personal Data, you must regularly review all the systems and processes under your control or responsibility 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.

16. DIRECT MARKETING

16.1 We are subject to certain rules and privacy laws when sending marketing communications to Data Subjects.

16.2 For example, a Data Subject's prior consent is required for electronic direct marketing (for example, if the Campaign wishes to send them communications by email or by text which encourage them to give us their support).

16.3 The right to object to direct marketing communications must be explicitly offered to the Data Subject in an intelligible manner each time they are contacted. That right must be offered in a way that is clearly distinguishable from other information in the communication.

16.4 A Data Subject's objection to direct marketing must be promptly honoured. If a customer 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.

17. SHARING PERSONAL DATA

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

17.2 The Office 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.

17.3 If you would like to share Personal Data with a third party, please first notify your supervisor, and if necessary, seek approval from the Head of Data Protection.

18. CHANGES TO THIS PRIVACY STANDARD

18.1 We keep this Privacy Standard under regular review. We may amend this Privacy Standard to reflect changes in Data Protection Legislation or our organisation. We will notify you of any changes and you will be deemed to have read and accepted any such changes if you continue to work with us.

18.2 This Privacy Standard does not override Data Protection Legislation or any other applicable national data privacy laws and regulations in countries which the Office is subject to.

Annex A

Definitions

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, signify agreement to the Processing of Personal Data relating to them.

Controller: the person or organisation that determines when, why and how to process Personal Data. We are the Controller of all Personal Data relating to our Office Personnel and Personal Data used in our business for our own commercial purposes.

Criminal Convictions Data: means personal data relating to criminal convictions and offences and includes personal data relating to criminal allegations and proceedings.

Data Protection Legislation: means any laws and regulations relating to privacy of the processing of personal data including the following legislation to the extent applicable or as may be revised, amended or superseded from time to time: (a) the Privacy and Electronic Communications Regulations; (b) the Data Protection Act 2018; and (c) the General Data Protection Regulation 2016/679 ("**GDPR**").

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

EEA: the 27 countries in the EU, and United Kingdom, Iceland, Liechtenstein and Norway.

Office Personnel: all employees, workers, contractors, agency workers, consultants, directors, members, volunteers and others.

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 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 leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

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 Office collects information about them.

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, destroying, transmitting or transferring it.

Special Categories of 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.

Supervisory Authority: an independent public authority which is established by a member state pursuant to Article 51 of the GDPR.