LAUNCHPAD FOR LITERACY

DATA PROTECTION POLICY / COMPLIANCE STATEMENT

1. Introduction

1.1 This Data Protection Policy ("**Policy**") sets out how Launchpad for Literacy (**"we", "our", "us", "Launchpad"**) handles Personal Data.

1.2 This Policy 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 clients, employees, applicants, consultants, contractors, suppliers etc.

1.3 This Policy applies to all Launchpad Personnel, who must read, understand and comply with this Policy. Compliance with this Policy is mandatory.

2. Personal Data protection principles

2.1 We adhere to the principles relating to the Processing of Personal Data set out in the GDPR which require Personal Data to be:

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

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

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

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

(v) 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**).

(vi) 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**).

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

(viii) 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**).

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 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.

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

(i) the Processing is necessary for the performance of a contract with the Data Subject;

(ii) to meet our legal compliance obligations;

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

(iv) to protect the Data Subject's vital interests (to protect someone's life); and/or

(v) to pursue our legitimate interests or those of a third party, but only where we use Personal Data in a way that the Data Subject(s) would reasonably expect and that has a minimal privacy impact. Where we rely on our legitimate interests as a lawful basis, the purposes must not prejudice the interests or fundamental rights and freedoms of Data Subjects. For example, if the Processing in question would cause unjustified harm to the Data Subject, our legitimate interests are likely to be overridden.

We will identify and document the legal ground being relied on for our Processing activities.

4. Consent

4.1 In the majority of cases, we do not rely on Consent as our legal basis for Processing Personal Data. Instead we issue a Privacy Notice to individuals whose data we Process (please see section 5 below).

4.2 A Data Subject consents to the Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires a positive action, meaning that 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.

4.3 Where relevant, we will need to keep records of all Consents so that we can demonstrate compliance with Consent requirements.

5. Transparency (notifying Data Subjects)

5.1 The GDPR requires us 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, which must be concise, transparent, accessible, and in clear and plain language so that a Data Subject can easily understand them.

5.2 We will maintain a GDPR-compliant Privacy Notice in a prominent position on our website and issue Privacy Notices to third parties directly, where practical.

6. Sensitive Personal Data and Criminal Convictions Data

When Processing Sensitive Personal Data, we must comply with data protection legislation. We do not currently Process Sensitive Personal Data.

7. 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. We do not use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless the

new purpose is compatible with our original purpose and we have informed the Data Subject of the new purposes, or they have Consented (where necessary).

8. Data minimisation and storage limitation

8.1 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed. Launchpad Personnel may only Process Personal Data when performing a job duty requires it.

8.2 It is important that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with our data retention policy.

9. Accuracy

It is important that we ensure the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. We must check the accuracy of any Personal Data at the point of collection and at periodic intervals afterwards.

10. Security, integrity and confidentiality

10.1 Protecting Personal Data

(i) 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 (including use of encryption where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

(ii) When sending documents that contain Personal Data by post, we ensure the envelope or packaging is well-sealed and we mark the front with "***Strictly private and confidential***" and ensure any USB sticks or discs containing Personal Data are password protected and send the password by alternative means.

10.2 Security measures for electronic records

(i) We shall ensure that all Launchpad devices have adequate protection against malicious software and/or viruses. We do not install software onto Launchpad devices without such software first being checked for viruses by our IT support.

(ii) All devices containing Personal Data are password protected. **We do not write down passwords or disclose them to anyone else.**

(iii) We do not allow personal devices to be used for work purposes.

(iv) We ensure Launchpad devices are locked when the device is left unattended.

(v) Access to electronic records containing Personal Data is restricted to Launchpad Personnel for whom access is necessary.

10.3 Security measures for manual records

(i) All manual records containing Personal Data must be kept securely.

(ii) Access to manual records containing Personal Data should be restricted to Launchpad Personnel for whom access is necessary.

(iii) When destroying documents in accordance with our data retention policy or otherwise, we ensure such documents are shredded without delay.

10.4 **Telephone enquiries**

If we receive telephone enquiries we are careful about disclosing any Personal Data held by us. In particular we:

(i) check the caller's identity to make sure that information is only given to a person who is entitled to it; and/or

(ii) suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked over the phone.

10.5 **Reporting a Personal Data Breach**

(i) The GDPR requires Data Controllers to notify ***certain*** Personal Data Breaches to the Information Commissioner's Office ("**ICO**") and, in certain instances, to the Data Subject.

(ii) If we know or suspect that a Personal Data Breach has occurred, we investigate this in a timely manner and preserve all evidence relating to the potential Personal Data Breach. If we decide the breach needs to be notified to the ICO and/or the individual, this must be done within 72 hours of us becoming aware of the breach.

(iii) We shall then take all reasonable steps to mitigate the risk of the Personal Data Breach causing any further damage including but not limited to:

- if relevant, contacting the unintended recipient to request deletion of the relevant document/e-mail and for confirmation of deletion;
- deciding whether the Personal Data Breach needs to be notified to the ICO based on all the circumstances, including whether the breach is likely to present a risk to the Data Subject's rights and freedoms;
- deciding whether the Personal Data Breach needs to be notified to the Data Subject based on all the circumstances, including whether the breach is likely to result in a high risk of adversely affecting the Data Subject's rights and freedoms; and
- investigating the causes of the breach and how the risks of such incidents happening again can be reduced.

11. Data Subject's rights and requests

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

(i) withdraw Consent to Processing at any time;

(ii) receive certain information about our Processing activities;

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

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

(v) 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;

(vi) restrict Processing in specific circumstances;

(vii) challenge Processing which has been justified on the basis of our legitimate interests;

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

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

(x) make a complaint to the ICO; and

(xi) receive or ask for their Personal Data to be transferred to a third party in a commonly used and machine readable format.

11.2 If we receive such a request from a Data Subject, we follow the below procedure:

(i) upon being notified of the request, take steps to investigate the identity of the individual making the request, with the assistance of relevant Launchpad Personnel;

(ii) upon satisfaction that the Personal Data being requested relates to the individual wishing to exercise his or her rights, confirm to the individual that Launchpad is progressing such request;

(iii) liaise with relevant Launchpad Personnel to identify the relevant Personal Data;

(iv) check whether any other individuals' rights and freedoms will be compromised by complying with the request, including whether any Personal Data needs to be redacted; and

(v) consider whether the request must be complied with in the context of Launchpad's other legal obligations and, if so, provide the information to the Data Subject or confirm to the Data Subject the request has been complied with.

We must comply with requests by Data Subjects to exercise the above rights without undue delay and in any event within one month of receiving the request and can only charge a fee in certain circumstances if the request is manifestly unfounded or excessive. In certain situations, we may refuse to comply with a request if it is excessive, but must explain the reason for the refusal to the individual and inform him or her of their right to complain to the ICO.

12. Accountability

12.1 Record keeping

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

These records should include, at a minimum, the name and contact details of the Data 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.

12.2 **Privacy By Design and Data Protection Impact Assessments**

We are required to implement a concept called “Privacy by Design” when Processing Personal Data. This involves implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with the GDPR.

When implementing such measures, we will take account of the following:

(i) the cost of implementation;

(ii) the nature, scope, context and purposes of Processing; and

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

When implementing major new systems within Launchpad, or carrying out the large scale Processing of Sensitive Personal Data, we must carry out a “Data Privacy Impact Assessment”. This involves identifying and reducing risks associated with Processing Personal Data.

Such Data Privacy Impact Assessments must include:

(i) a description of the Processing, its purposes and our legitimate interests if appropriate;

(ii) an assessment of the necessity and proportionality of the Processing in relation to its purpose;

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

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

12.3 **Direct marketing**

We are subject to certain rules and privacy laws when marketing to third parties.

For example, a Data Subject's prior consent is required for electronic direct marketing (e.g. by email). The limited exception for existing clients known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

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, such as an “opt-out” link on all electronic communications.

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

13. Implementation

We will regularly review this policy and our data protection practices more generally.

We will ensure that all Launchpad Personnel are trained on data protection matters in line with this Policy and as part of the induction process.

14. Definitions

Consent: freely given, specific, informed and unambiguous agreement by the Data Subject to the Processing of their Personal Data. Consent must be made by a clear and positive action and cannot be implied.

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

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 used for our activities.

Data Subject: a living, identified or identifiable individual about whom we hold 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*), together with the Data Protection Act 2018. Personal Data is subject to the legal safeguards specified in the GDPR and the DPA 2018.

Launchpad Personnel: all employees, volunteers, applicants, consultants, contractors etc. of Launchpad.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify from that data alone or in combination with other information we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Criminal Convictions Data.

Personal Data Breach: any act or omission that compromises the security or confidentiality of Personal Data or the physical or technical safeguards that we or our third-party service providers put in place to protect such Personal Data. The loss, unauthorised access or disclosure of Personal Data is a Personal Data Breach.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when Launchpad collects and Processes 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, disclosing, or destroying it. Processing also includes transferring Personal Data to third parties.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual orientation, biometric or genetic data and Criminal Convictions Data.