Amala Data Protection Policy

1. Introduction

This policy sets out how Amala Education ("Amala", "we", "our", "us") handle the personal data of individuals. In order to carry out our work, Amala needs to collect and use certain types of personal data about various individuals, including employees, students, volunteers, supporters, service users and other individuals with whom we interact ("data subjects"). This personal data must be collected and dealt with appropriately, whether it is collected on paper, stored in an electronic database, or recorded on other material.

As a limited company in the UK, Amala operates under UK data protection law. This policy sets out Amala's top level approach to the UK General Data Protection Regulation ("**UK GDPR**"), the Data Protection Act 2018 ("**DPA**") and associated laws. This policy is complemented by specific privacy policies, statements and training for different activities undertaken by Amala so there are appropriate safeguards that ensure that the processing of personal data is carried out appropriately under the UK GDPR. Everyone processing personal data must understand that they are contractually responsible for following good data protection practice.

This Data Protection Policy applies to all of our employees, workers, contractors, agency workers, consultants, directors, members and others ("you", "your"). You must read, understand and comply with this Data Protection Policy when processing personal data on our behalf and attend training on its requirements. This Data Protection Policy sets out what we expect from you for us to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. Any breach of this Data Protection Policy may result in disciplinary action. You are required to familiarise yourself with this policy.

This Data Protection Policy is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the Data Protection Manager.

2. Scope

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. We are exposed to potential fines of up to £17.5 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 UK GDPR.

The Data Protection Manager is responsible for overseeing this Data Protection Policy. That post is held by Co Executive Director Polly Akhurst, and she is responsible for Amala's

compliance with the UK GDPR, training staff and volunteers appropriately and responding to requests from the Information Commissioner's Office, constituents or data subjects.

Please contact Polly Akhurst on polly@amalaeducation.org with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed. In particular, you must always contact the Data Protection Manager 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 used by us);
- if you need to rely on consent and/or need to capture explicit consent;
- if you need to draft privacy notices or privacy policies;
- if you are unsure about the retention period for the personal data being processed;
- if you are unsure about what security or other measures you need to implement to protect personal data;
- if there has been a personal data breach;
- if you are unsure on what basis to transfer personal data outside the UK;
- if you need any assistance dealing with any rights invoked by a data subject;
- whenever you are engaging in a significant new, or change in, processing activity which is likely to require a Data Privacy Impact Assessment or plan to use personal data for purposes other than what it was collected for;
- if you plan to undertake any activities involving automated processing including profiling or automated decision-making;
- if you need help complying with applicable law when carrying out direct marketing activities; or
- if you need help with any contracts or other areas in relation to sharing personal data with third parties (including our vendors).

3. Personal Data Protection Principles

We adhere to the principles relating to processing of personal data set out in the UK GDPR which require personal data to be:

- Processed lawfully, fairly and in a transparent manner in relation to the individual ('**lawfulness, fairness and transparency**')
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with this ('**purpose limitation**')
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**')
- Accurate and, where necessary, kept up to date ('**accuracy'**)
- Kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data are processed ('**storage limitation**')

- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('**integrity and confidentiality**')
- Not transferred to another country without appropriate safeguards being in place ('**transfer limitation**'); and
- 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**').

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

4. Lawfulness, Fairness, Transparency

Lawfulness:

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 UK 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.

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

- The data subject has given their **consent** to the processing;
- The processing is **necessary for the performance of a contract** to which the data subject is a party or for the taking of steps at the request of the data subject with a view to entering into a contract;
- The processing is **necessary for compliance with any legal obligation** to which Amala is subject, other than an obligation imposed by contract;
- The processing is **necessary in order to protect the vital interests** of the data subject; and/ or
- The processing is **necessary for the purposes of legitimate interests** pursued by Amala or by the third party or parties to whom the personal data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

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

Consent:

A controller must only process personal data on the basis of one or more of the lawful bases set out in the UK GDPR, which include consent.

Where processing personal data requires consent, Amala will ensure that it provides sufficient information to the data subject, so as to make sure the consent is specific and informed, that it is genuinely and freely given, and that it involves a documented, affirmative action on the part of the data subject. Amala will consider the following points to design the necessary procedures and privacy statements for each type of processing where consent is required:

- The data subject has received sufficient information on and clearly understands why their data is needed, how it will be used, and what for;
- The data subject understands what the consequences are, should they decide not to give consent to processing;
- The data subject grants affirmative written or verbal consent for data to be processed (it will not be implied);
- The data subject is competent enough to give the consent described above, and has given this freely without any duress;
- Amala will also consider what other information should be included in any specific privacy notices/statements in order for data subjects to feel empowered and aware of how their personal data is used by Amala; and
- If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

Amala understands that it must only process personal data for the specific purposes for which it was collected. Amala will not process personal data for purposes other than or additional to those it was collected for and which were identified in the relevant privacy statement or other documents provided to the data subject.

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.

When processing Special Category 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), 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.

You will need to evidence consent captured and keep records of all consents so that we can demonstrate compliance with consent requirements.

Transparency:

The UK GDPR requires 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.

Whenever we collect personal data directly from data subjects, including for HR or employment purposes, we must provide the data subject with all the information required by the UK GDPR including the identity of the controller and Data Protection Manager, 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.

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 UK 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 UK GDPR and on a basis which contemplates our proposed processing of that personal data.

If you are collecting personal data from data subjects, directly or indirectly, then you must provide data subjects with a privacy notice.

5. Accuracy

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

Amala will actively encourage data subjects to keep their personal data up to date and accurate, and will ensure that there are easy methods by which they can do this, such as by clicking on ‘update your preferences’ on the Amala mailing list, or by contacting Amala directly via email on hello@amalaeducation.org

Amala will also ensure it undertakes appropriate checks to ensure personal data is kept up to date and accurate.

6. 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 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. 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. As such, different time periods for retention will apply depending on the type of personal data and the reason for its processing.

We 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 that data to be kept for a minimum time.

In general, personal data will be stored for around six years after our last interaction with the individual, as this corresponds to the amount of time generally that there may be a challenge or dispute for which the personal data may be relevant. Donor data will be stored for six years, in compliance with HMRC requirements relating to Gift Aid.

Data of Amala alumni will be held for longer for the purposes of alumni engagement (including updates about Amala and educational and training opportunities that may be of interest) and evaluating the impact of the Amala programme (via surveys, with their consent), unless individual rights relating to deletion of that data are exercised. Amala considers this appropriate so that its alumni may corroborate their education with Amala in the future and because alumni will have a legitimate interest in hearing from Amala. Only the minimum amount of personal data required for these purposes will be kept.

You will take all reasonable steps to destroy or erase from our systems all personal data that we no longer require in accordance with our applicable records retention schedules and policies. This includes requiring third parties to delete that data where applicable.

You 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.

8. Security, Integrity and Confidentiality

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

Amala will implement appropriate security measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, including through the transmission or storage on or within a network.

These security measures will include:

- Industry standard firewall and other network security features such as well encrypted cloud or physical server systems;
- Clear guidelines for staff and volunteers on device and network security expectations placed on them;
- Robust data backup and recovery processes provided by leading industry suppliers; and
- Periodic security audits of online systems.

We will regularly evaluate and test the effectiveness of these security measures to ensure the 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 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; and
- Availability means that authorised users are able to access the personal data when they need it for authorised purposes.

9. Reporting a Personal Data Breach

The UK GDPR requires controllers to notify any personal data breach to the Information Commissioner and, in certain instances, the data subject.

We may also need to notify the Charity Commission.

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, do not attempt to investigate the matter yourself. Immediately contact the person or team designated as the key point of contact for personal data breaches and follow our Data Breach Response Plan. You should preserve all evidence relating to the potential personal data breach.

10. 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 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;
- request a copy of an agreement under which personal data is transferred outside of the UK;
- object to decisions based solely on automated processing, including profiling (automated decision making);
- 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; and

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 Data Protection Manager.

11. Transfer Limitation

The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK 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 may only transfer personal data outside the UK if one of the following conditions applies:

- the UK has issued regulations 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;
- appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved for use in the UK, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the Data Protection Manager;
- the data subject has provided explicit consent to the proposed transfer after being informed of any potential risks; or
- the transfer is necessary for one of the other reasons set out in the UK 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. 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 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;
- the transfer complies with any applicable cross-border transfer restrictions; and

- a fully executed written contract that contains UK GDPR-approved third party clauses has been obtained.

13. Data Protection Impact Assessments

Where we intend to use personal data in a more intrusive way we must carry out an initial assessment to consider whether the use is justified. Carrying out a Data Protection Impact Assessment (DPIA) helps us identify and minimise the privacy risks associated with the use of personal data when implementing major system or business change programs including:

- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- automated processing including profiling and automated decision making;
- large-scale processing of special categories of personal data; and
- large-scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

- a description of the processing, its purposes and the controller's legitimate interests if appropriate;
- an assessment of the necessity and proportionality of the processing in relation to its purpose;
  an assessment of the risk to individuals; and
  the risk mitigation measures in place and demonstration of compliance.

14. Accountability

The controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

Amala must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

- appointing a suitably qualified Data Protection Manager and an executive 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 including this Data Protection Policy or privacy notices;
- regularly training our personnel on the UK GDPR, this Data Protection Policy and data protection matters including, for example, data subject's rights, consent, legal

basis, DPIA and personal data breaches. We must maintain a record of training attendance by our 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.

15. Record Keeping

The UK 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, the name and contact details of the controller and the Data Protection Manager, 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.

16. 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 undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training.

You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of personal data.

17. Adopting privacy by design

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.
We must ensure that any privacy settings are by default set to the most privacy protective setting. We must ensure that the minimal amount of personal data is collected and used through our technology.

You must assess what Privacy by Design measures can be implemented on all programmes, systems or 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.

As far as possible we should employ pseudonymised datasets to reduce risk to individuals' privacy.

18. Automated processing 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 special categories of personal data are being processed, then grounds (b) or (c) will not be allowed but the special categories of 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.

A DPIA must be carried out before any automated processing (including profiling) or automated decision making activities are undertaken.

19. Direct Marketing

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

For example, a data subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers 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.

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.

20. Changes to this Data Protection Policy

We keep this Data Protection Policy under regular review.

This version was last updated in March 2022.
This Data Protection Policy does not override any applicable national data privacy laws and regulations in countries where Amala operates.

21. Related Policies and Procedures

Complaints Polic
Disciplinary Policy and Procedures
Safeguarding and Welfare Policy
Team Code of Conduct
Whistleblowing Policy

22. Acknowledgment of Receipt and Review

Data Protection Policy and Procedure
Policy Owner: Co-Executive Director (Polly Akhurst)
Approved by: Amala Board of Trustees
Effective from: 28 September 2018
Last revision: 10 June 2023

I, [NAME], acknowledge that on [DATE], I received and read a copy of Amala's Data Protection Policy and understand that I am responsible for knowing and abiding by its terms.

Signed …….
Printed Name …….
Date …….