ROBIN HOOD
MULTI ACADEMY TRUST
www.robinhoodmat.co.uk

DATA PROCESSOR AGREEMENT

Dear Supplier,

As you will know, the GDPR took effect on 25th May 2018, and your company presently processes data about 'subjects' at the school – that may be about parents/carers, students or our workforce.

The purpose of writing to you now is that, as the data controller, we want to ensure that the way that your organisation takes care of the data we share with you complies with the obligations of the GDPR.

The following terms will therefore apply with immediate effect and replace any relevant data processing clauses in the existing contracts between us.

The objective is also to help to protect against the possibility of changes being made to the scope of the processing over time without taking into account any additional risks this poses to the data subjects.

Recital 81 of the GDPR is clear that, in agreeing the contract or other legal act, the specific tasks and responsibilities of your company and the risk to the rights and freedoms of the data subjects must be taken into account.

Under Article 28.3(a):

- your company may only process personal data in accordance with our written instructions (including when making an international transfer of personal data) unless required to do so by law; this doesn't prevent your company from complying with any other laws that you may be subject to.

Under Article 28.3(b):

- Your company must obtain a commitment of confidentiality from anyone it allows to process the personal data, unless they are already under such a duty by law. This includes your company's employees as well as any temporary workers and agency workers.

Under Article 28.3(c)

- your company is subject to the same Article 32 requirements as the School is to keep secure the personal data it is processing. These include adopting security measures including encryption, pseudonymisation, resilience of processing systems and backing up personal data in order to be able to reinstate the system.

Under Article 28.3(d):

- your company should not employ another company without our prior specific or general written authorisation;
- if another company is employed under your prior general written authorisation, your company should let you know of any changes it has made and give you a chance to object to them;
- if your company employs another company, then it must impose the contract terms that are required by Article 28.3 of the GDPR on the sub-company;
- and if your company employs another company, then the your company will still be liable to you for the compliance of the subcompany.

Under Article 28.3(e):

- your company must assist us in meeting our obligations to data subjects under chapter III of the GDPR, by having appropriate technical and organisational measures.

Under Article 28.3(f) taking into account the nature of the processing and the information available to your company:

- your company must assist us in meeting our Article 32 obligation to keep personal data secure;
- your company must assist us in meeting our Article 33 obligation to notify personal data breaches to your supervisory authority;
- your company must assist you in meeting your Article 34 obligation to advise data subjects when there has been a personal data breach;
- your company must assist you in meeting your Article 35 obligation to carry out data protection impact assessments (DPIAs); and
- your company must assist you in meeting your Article 36 obligation to consult with your supervisory authority where your DPIA indicates there is an unmitigated high risk to the processing.

Under Article 28.3(g):

- at the end of the contract your company must, at our choice, either delete or return to you all the personal data it has been processing for you; and
- an exception to this general rule applies if your company is required to retain the personal data by law.

Under Article 28.3(h):

- your company must provide you with all the information that is needed to show that that both of you have met the obligations of Article 28;
- your company must submit and contribute to audits and inspections that you carry out, or another auditor appointed by you carries out; and
- your company must tell us immediately if it thinks it has been given an instruction which doesn't comply with the GDPR, or related data protection law.

As this is new legislation, the ICO may publish new guidance and further contractual updates may be issued.

In order for the school to continue using your company's services, we require your written agreement within 14 days of the date of this email. I therefore request that you complete the acknowledgement attached to confirm that your organisation is GDPR compliant and that you have ongoing processes and checks in place to ensure compliance is maintained.

Failure to do so may result in termination of the contract between us.

I look forward to your cooperation in this matter.

John McDermott
Data Protection Manager
E: gdpr@robinhoodschool.co.uk

Robin Hood Multi Academy Trust
77 Pitmaston Road, Hall Green, Birmingham, B28 9PP
W: www.robinhoodmat.co.uk
T: 0121 464 2187

Robin Hood Multi-Academy Trust: A company limited by guarantee
Registered in England: Company Number: 08686006

Company Name:

Dear Trustees of Robin Hood Multi-Academy Trust

Re: GDPR Compliance

I confirm that …….. (Organisation) is GDPR compliant and that there are processes in place to ensure ongoing compliance through regular audit and procedural check. I confirm that the organisation is registered with the Information Commissioner's Office.

I confirm that any personal / sensitive data held on behalf of Robin Hood Multi-Academy Trust and its schools is held in compliance with the GDPR regulations, held securely and used only in relation to the agreement in place to provide services to the school. Any data no longer required will be destroyed securely and in line with the required retention arrangements under GDPR.

Yours faithfully

On behalf of …….

Name:

Position:

Date: