# Blue Gate Fields Infant School

# GDPR Compliant Agreement for Suppliers

---

Last updated: 22 February 2018

## Introduction

To ensure compliance with the General Data Protection Regulation (GDPR), and that both schools and suppliers understand the terms under which data will be shared, maintained and securely deleted, an agreement should be constructed outlining the terms and conditions of both parties' approach to data protection. This document outlines the purpose and terms of a data processing agreement, where the school is the data controller and **name of supplier** …….. is the data processor.

This document complies with the requirements set out in the GDPR, which will come into effect on 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

## Definitions

For the purpose of this agreement:

- **Processing** – Is any operation or set of operations performed on personal data or sets of personal data, whether by manual or automated means. This can include collecting, recording, organising, structuring, storing or adapting data.

- **Data controller** – Is the person, public authority, agency or other body which alone, or jointly with other parties, determines the purposes and means of the processing of personal data.

- **Data processor** – Is a person or organisation who processes data on behalf of the data controller.

- **Data protection officer (DPO)**– Refers to the designated person who oversees the proper care and use of data, including personal data and sensitive personal data.

- **Personal data** – Is any information relating to an identified or identifiable person; an identifiable person is someone who can be identified by reference, e.g. a name, identification number or physical trait.

- **Sensitive personal data** – Refers to personal data which reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, details of someone's health or sexual life, or their genetic data.

- **Data breaches** – Is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

- **Secure disposal** – Is the safe deletion or destruction of all personal or sensitive personal data.

## 1. Purpose

1.1. This agreement, between **Blue Gate Fields Infant School** (data controller) and **supplier name:** ……. (data processor) outlines the terms under which the two parties agree to share data under the GDPR.

1.2. The parties acknowledge that under the GDPR **Blue Gate Fields Infant School** is a data controller and **supplier name:** ……. is the data processor. There could be cases of the school and the supplier being Joint Data Controllers.

1.3. This agreement ensures both parties have a clear framework to work to, and act in compliance with the needs and requirements of one another and the GDPR.

1.4. The school and supplier understand that data sharing is necessary in order for the data processor to fulfil its obligations to the data controller.

1.5. This agreement clearly identifies the DPOs from both parties and ensures they understand their roles in protecting data and in relation to upholding this agreement. The DPO's from both parties may also review the Data Mapping and GDPR audits of the other party and this must be provided in a timely manner.

1.6. To ensure the security of data remains a high priority, both parties will review each other's data protection policies in order to reach an agreement that benefits the data controller and processor equally.

## 2. The data controller

2.1. The data controller will, in accordance with Article 24 of the GDPR, take into account the nature, scope, context and purposes of processing; as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.

2.2. The data controller, in collaboration with the data processor, shall implement appropriate measures, e.g. up-to-date security software and consistent reviewing procedures, to ensure they are able to demonstrate that processing is performed in accordance with the GDPR. These measures will be reviewed and updated where necessary.

2.3. The data controller's roles and procedures will be set out in their **GDPR Data Protection Policy**.

2.4. Data controllers remain directly liable for compliance with all aspects of the GDPR and for demonstrating that compliance. If this isn't achieved, the data controller may be liable to pay damages in legal proceedings or be subject to fines or other penalties and corrective measures.

## 3. The data processor

3.1. The data processor will adhere to, update and review the **GDPR Data Protection Policy** they have implemented.

3.2. Under Article 28 of the GDPR the data processor shall not engage another processor without prior knowledge, or written authorisation of the data controller.

3.3. The data processor will only process the personal data they are told to by the data controller, unless instructed otherwise by law.

3.4. The data processor will ensure that the persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.5. The data processor will assist the data controller by putting in place the appropriate measures to fulfil the data controller's obligations to respond to requests for exercising the data subject's rights.

3.6. The data processor will delete or return all personal data to the data controller at their request, once the contract reaches its termination.

3.7. The data processor will, at the request of the data controller, make available all information necessary to demonstrate compliance with the obligations set out in Article 28 of the GDPR, and allow for a contribute to audits and inspections conducted by the data controller or another auditor mandated by the data controller.

3.8. The data processor will immediately inform the data controller if they believe an instruction they have given breaches the GDPR or any other data protection law.

3.9. In the event the data processor engages another data processor for carrying out specific data processing activities on behalf of the data controller, the same data protection obligations will apply. If the other data processor fails to fulfil its data protection obligations, the initial data processor will remain fully liable to the data controller for the performance of the other data processor's obligations.

3.10. The data processor will adhere to an approved code of conduct and be suitably qualified in order to guarantee the role can be fulfilled competently and to the satisfaction of the data controller in compliance with the GDPR.

## 4. Processing and record keeping

4.1. The legal basis for processing data will be identified and agreed on by the data protection officer DPOs from **Blue Gate Fields Infant School** and **supplier name:** _____

| Organisation | Name of DPO | Phone number | Email address |
|---|---|---|---|
| Blue Gate Fields Infant School | EduAction Limited | 02077903611 (School) | info@EduAction.org.uk |
| **Name of supplier** | | | |

4.2. The data that data processor will keep includes: Staff details

4.3. Data will not be kept for longer than its purpose(s), as agreed by the data controller and data processor.

4.4. Unrequired data will be deleted as soon as practicable.

4.5. Some records, such as those relating to former pupils or employees of the school, may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

4.6. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data is no longer required, or has fulfilled its purpose(s).

4.7. DPOs from both parties will meet yearly to discuss whether any data can be destroyed.

4.8. Once the contract ends, the data shared by the data controller and data processor will be securely disposed of.

## 5. Data security

5.1. The security measures in place to ensure effective protection of physical data include: e.g. locked filing cabinets, drawers or safes with restricted access.

5.2. The security measures in place to ensure effective protection of digital data include: e.g. password-protected hard drives and encrypted portable devices.

5.3. Confidential paper records will be kept e.g. in a locked filing cabinet.

5.4. Confidential paper records will not be left unattended or in clear view anywhere with general access.

5.5. Where data is saved on a portable device, the device will be kept e.g. in a locked cupboard.

5.6. Digital data is password-protected, coded or encrypted on local hard drives and on a network drive that is regularly backed up and maintained.

5.7. Portable devices will not be used to hold personal information unless they are password-protected and fully encrypted.

5.8. All electronic devices are password-protected to secure the information on the device in case of theft.

5.9. Data processors will update and review security measures in accordance with their **GDPR Data Protection Policy**.

5.10. Under no circumstances does the data processor allow any unauthorised persons to access confidential or personal information.

5.11. The physical security of the data processor's buildings and storage systems, and access to them, is reviewed on a yearly basis.

5.12. All data, physical or digital, pertaining to photographs or videos, will be securely disposed of three months after their creation.

## 6. Data breaches

6.1. The DPOs will take steps to ensure that all staff members from both parties are made aware of, and understand, what constitutes a data breach as part of their training.

6.2. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority, e.g. ICO, will be informed by the data controller/processor as soon as possible.

6.3. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it.

6.4. Any breaches will be fully investigated by the DPOs from both parties and security measures will be assessed and reviewed in relation to the investigation.

6.5. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the data controller / processor will notify those concerned directly.

6.6. If the data controller and data processor agree that a breach is sufficiently serious, the public will be notified without undue delay.

6.7. The data controller and data processor understand that failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

## 7. Agreement

7.1. By signing this agreement **Blue Gate Fields Infant School** (data controller) and **name of supplier**:…… (data processor) agree to adhere to the terms set out in this agreement one school academic year.

7.2. In the event a new DPO is employed by either **Blue Gate Fields Infant School** or **name of supplier**:……, this agreement will be reviewed and re-signed to ensure all parties remain knowledgeable of their expectations in relation to this agreement.

Data controller signed

| Job title | Name | Signed | Date |
|---|---|---|---|
| **Headteacher** | | | |
| **DPO** | | | |

Data processor signed

| Job title | Name | Signed | Date |
|---|---|---|---|
| **Director** | | | |
| **DPO** | | | |