Managing Sub Contractors and 3rd Parties Process

Nov 2020

Version	1.0
Date Approved by Governors:	10th Nov 2020
Review date:	10th Nov 2022
Version History	

1. Scope

All external suppliers that process personal data on behalf of Fairfield School are within the scope of this procedure.

2. Responsibilities

2.1 The Business/Officer Manager / Data Protection Officer in conjunction with the Finance Department are responsible for approving the selection of all sub-contracted processors of personal data in line with the requirements of this procedure.

2.2 The owners of third-party relationships are responsible for ensuring that all data processing is carried out in line with this procedure.

2.3 The IT Manager is responsible for ensuring that adequate technical and other resources that might be required are made available to support the relationship owner in the monitoring and management of the relationship.

2.4 The Business/Office Manager is responsible for carrying out regular audits of contractor or third-party compliance.

3. Procedure

3.1 Fairfield School selects only suppliers that can provide technical, physical and organisational security that meet Fairfield School's requirements in terms of all the personal information they will process on Fairfield School's behalf.

3.2 Suppliers from outside the EU will only be selected under the following conditions, in addition to the conditions noted elsewhere in this procedure.

3.2.1.1 If the supplier or the state in which it resides has been positively identified in an adequacy decision by the EU Commission; or

3.2.1.2 Where there are legally binding corporate rules, and organizational and technical safeguards, established between Fairfield School and the supplier to secure the rights and freedoms of data subjects at least equal to those afforded within the EU; or

3.2.1.3 Where the arrangement has been approved by the Information Commissioner.

3.3 An information security risk assessment, is carried out before a supplier is engaged (See **Annex A**) and, if the Data Protection Officer / Business Manager considers it necessary because of the nature of the personal information to be processed or because of the particular circumstances of the processing, an audit of the supplier's security arrangements against the requirements of Cyber Essentials may be conducted before entering into the contract.

3.4 Fairfield School requires a written agreement (See **Annex B**) to provide the service as specified and requires the supplier to provide appropriate security for the personal information it will process.

3.5 All data processing contracts allow Fairfield School to conduct regular audits of the supplier's security arrangements during the period in which the supplier has access to the personal information.

3.6 All data processing contracts forbid suppliers from using further subcontractors without Fairfield School's written authorization for the processing of personal information.

3.7 Contracts with second-level subcontractors will only be approved if they require the subcontractors to comply with at least the same security and other provisions as the primary subcontracting organisation (the supplier) if they specify that, when the contract is terminated, related personal information will either be destroyed or returned to Fairfield School.

This policy will be reviewed on a bi-annual basis.

DRAFT LETTER AND INFORMATION SECURITY QUESTIONNAIRE FOR SUB CONTRACTORS AND 3RD PARTIES

Date:

[Insert Supplier Name and Address}

Dear Sir/Madam,

GDPR Compliance

As an Academy we are continually working towards ensuring compliance with the GDPR and amended Data Protection Act that came into force on 25 May 2018.

As a sub-contractor or 3rd party supplier you need to confirm that you have undertaken the necessary review of your processes and procedures to comply with the changes. To continue with our commercial relationship, we need confirmation of this and agreement that the current contract or arrangements will be agreed and amended to reflect this.

Please complete the series of questions below and explain how you will comply.

We require the form to be completed, signed and returned to us. We reserve the right to request any additional information from you about your processes and procedures that will enable us secure compliance with the GDPR requirements.

As a public authority we have an obligation to be compliant with GDPR and to demonstrate compliance.

Thank you for your assistance.

Kind regards

[Insert Name and Job Title of person signing the letter]

School name:

To comply our arrangements with you after 25 May 2018 must ensure that you will:

Supplier Requirement	**Confirm consent and process**
Only use the data we provide or that you access from our organisation in accordance with our instructions,	
Ensure that anyone in your organisation understands that and data they have access to or use about our students or staff is confidential and must not be shared with anyone without our prior agreement	
Take all steps to keep the data secure, whether it is paper records, emails, digital or electronic. Please note we reserve the right to ask for evidence and details about how this is done.	
If you sub contract any part of the task, and personal information and data is required by that sub-contractor, you will seek and obtain our consent before proceeding.	
On occasion, we may receive a request to release information that we hold about an individual, whose data you have used or processed on our behalf. Please confirm that in those situations you will co-operate with us and provide all records about the person within a specified timeframe.	
Should there be a data breach, please confirm that you will notify us as soon as you are aware.	
In the event of a breach please confirm that you will co-operate with us to report, manage and recover data that you have also had access to or use.	
In the event of a data breach, what is the process?	
You notify us if a breach occurs, as soon as you become aware of it.	
That you will delete or return (at our choice) all personal data at the end of the agreement	

(unless storage is required by EU/member state law);	
You will make available to the us all information necessary to demonstrate compliance; allow/contribute to audits (including inspections)	
Please provide answers to the following	
What processes do you have in place for testing the security of your system?	
When was this security system last tested and what was the outcome?	
What is your School's strategy for achieving compliance with the GDPR?	
Please provide details of your Data Protection/Information Security/Cyber Security Policy as appropriate	

I, …… on behalf of

…… confirm that the responses above are accurate and agree that this forms a written agreement and amendment to our current arrangement or contract with effect from 25 May 2018.

Signed…….

Dated……...

Role within organisation……...

Annex B to Managing Sub-Contractors and 3rd Parties Process

DRAFT LETTER AND AGREEMENT WITH SUB CONTRACTORS AND 3RD PARTIES

Dear [Insert Supplier Name],

DATA PROCESSOR AGREEMENT

We refer to the arrangement under which you (as the "**Supplier**") provide services to Fairfield School ("**we**", "**us**", and "**our**"), including the terms and conditions applicable to that arrangement (as updated and amended from time to time) (the "**Terms**").

With effect from 25th May 2018, the General Data Protection Regulation (Regulation (EU 2016/679) (the "**GDPR"**) replaces the Data Protection Act 1998 (the "**DPA**") in regulating the processing of personal data.

As part of our arrangement, we will be forwarding data to you that must be processed in accordance with all applicable Data Protection Laws (including the DPA and, from 25th May 2018, the GDPR).

Article 28(3) of the GDPR specifies certain provisions which must be included in contracts between "controllers" and "processors" (such terms are defined in both the DPA and the GDPR). As such, this letter sets out the agreement between us to ensure the protection and security of data which we pass to you for processing.

Linked to this, you acknowledge that we are the data controller in respect of any personal data that you process in the course of providing services for us.

AGREEMENT

In consideration for us forwarding to you such data, you agree to comply with all applicable Data Protection Laws and to use your best endeavours to ensure that by your actions you do nothing to compromise Fairfield School with the applicable Data Protection Laws.

With effect from the date of this letter, you confirm that:

1. The Data Protection Agreement and its Appendix at Annex 1 to this letter ("**Annex 1**") shall form a part of the Terms.

2. The provisions of Annex 1 shall replace any provisions in the Terms which expressly conflict, or are inconsistent, with any provisions of Annex 1. If there is any ambiguity between the provisions of the Terms (excluding this Data Processor Agreement) and this Data Processor Agreement, the provisions of this Data Processor Agreement shall prevail.

3. Except as set out in this letter, the Terms shall remain unchanged and shall continue in force.

NEXT STEPS

Please confirm the categories of personal data and data subjects in the Appendix to the Data Protection Agreement before signing and returning the enclosed copy of this letter (including a full copy of Annex 1) to acknowledge your agreement.

Yours faithfully

Signed ……

Name

For and on behalf of Fairfield School

Date ……

We agree to the provisions of the GDPR Addendum and the variation of the Agreement with effect from the Variation Date on the terms set out above.

Signed ……

Name ……

For and on behalf of ……

Date ……

Annex 1 – Data Protection Agreement

1. Definitions and interpretation

1.1 In this Agreement, unless the context otherwise requires, the following terms shall have the meanings set out below:

(a) "**School Personal Data"** means the Personal Data that you process on behalf of us under or in connection with the Terms;

(b) **"Data Protection Laws"** means all applicable data protection and privacy legislation, regulations and binding codes of practice issued by any DP Regulator, including the Data Protection Act 1998 and or 2018 (the "**DPA"**) and from 25th May 2018 Regulation (EU) 2016/679 (the **"GDPR"**); the Privacy and Electronic Communications (EC Directive) Regulations 2003; and all legislation enacted in the UK in respect of the protection of Personal Data; in each case, to the extent in force, and as such are updated, amended, re-enacted or replaced from time to time;

(c) **"DP Regulator"** means any governmental or regulatory body or authority with responsibility for monitoring or enforcing compliance with the Data Protection Laws;

(d) **"Services"** means the products and/or services provided by you under the Terms and more particularly set out in the background to this Agreement;

(e) **"Standard Contractual Clauses"** shall mean the Standard Contractual Clauses annexed to the European Commission Decision (2010/87/EU);

(f) **"Terms"** means all terms applicable to the legal relationship existing between the parties, including those individually negotiated and subject to written agreements, and under which you and your affiliates are hereafter identified as the "**Supplier**".

1.2 The terms **Data Subject**, **Personal Data**, **Personal Data Breach** and **processing** shall have the

meanings set out in the GDPR.

2. **Data protection**

2.1 The parties shall comply with the provisions and obligations imposed on them by the Data Protection Laws at all times when processing the School Personal Data in connection with the Terms.

2.2 The details of the processing of the School Personal Data carried out by the Supplier on our behalf are set out in the Appendix to this Agreement and form part of this Agreement (the "**Processing Instructions**").

2.3 Each party shall at all times maintain accurate, complete and up-to-date written records of all processing operations under its responsibility that contain at least the minimum information required by the Data Protection Laws and shall make such information available to any DP Regulator on request.

2.4 The Supplier shall:

(a) process the School Personal Data only for the performance of the Services in accordance with the Terms and the Processing Instructions and/or our other written instructions from time to time;

(b) ensure that all of its employees, officers, staff, agents and sub-contractors who have access to the School Personal Data are informed of the confidential nature of the School Personal data and are subject to appropriate contractual obligations of confidentiality when processing such School Personal Data;

(c) implement and maintain technical and organisational measures and procedures to preserve the confidentiality and integrity of the School Personal Data and ensure an appropriate level of security for the School Personal Data, including protecting the School Personal Data against the risks of accidental, unlawful or unauthorised processing, destruction, loss, alteration, disclosure, dissemination or access;

(d) only appoint a third party (including any subcontractors and affiliates) to process the School Personal Data with our prior written consent;

(e) where the Supplier sub-contracts any of its obligations to a sub-contractor who has been approved by us in accordance with clause 2.4(d), the Supplier shall enter into contractual data processing provisions with the sub-contractor, equivalent to those in place between the Supplier and us under this Agreement, for the duration of the sub-contractor's Processing of the School Personal Data.

(f) not transfer the School Personal Data outside the European Economic Area without our prior written consent and, where we provide such consent, the Supplier shall take such further actions as we direct (including entering into the Standard Contractual Clauses) to ensure that the transfer is subject to adequate safeguarding measures;

(g) inform us without undue delay if the School Personal Data is (while within the Supplier's or its subcontractors' or affiliates' possession or control) subject to a Personal Data Breach or is otherwise lost or destroyed or becomes damaged, corrupted or unusable;

(h) at our sole option, including on termination or expiry of the Terms or any part of them, return or irretrievably delete all the School Personal Data from all of the Supplier's software and/or hardware systems and, if applicable, procure that the School Personal Data is deleted from the software and/or hardware systems of the Supplier's employees, officers, staff, agents or subcontractors (as applicable) and not make any further use of the School Personal Data;

(i) at no additional cost, provide or make available to us and any DP Regulator such information and assistance as is reasonably required to verify, demonstrate or ensure compliance with the Supplier's obligations (and each subcontractor's obligations, if applicable) in this Agreement and/or the Data Protection Laws;

(j) take such steps as are reasonably required to assist us in ensuring compliance with our obligations under Articles 30 to 36 (inclusive) of the GDPR;

(k) notify us within two (2) Business Days if it receives a request from a Data Subject to exercise its rights under the Data Protection Laws in relation to that Data Subject's Personal Data;

(l) provide us with such co-operation and assistance as may reasonably be required in relation to any request made by a Data Subject to exercise its rights under the Data Protection Laws in relation to that Data Subject's Personal Data; and

(m) not disclose any School Personal Data to any person or Data Subject other than at our written request or as expressly provided for in the Terms.

2.5 At our request and provided that we shall enter into appropriate confidentiality agreements (as reasonably required by the Supplier), the Supplier shall permit us or our representatives to access any relevant premises, personnel or records of the Supplier on reasonable notice to audit and otherwise verify the Supplier's compliance with its obligations under this this Schedule and the Data Protection Laws.

2.6 If either party receives any complaint, notice or communication which relates directly or indirectly to the processing of the School Personal Data by the other party or to either party's compliance with the Data Protection Laws, it shall as soon as reasonably practicable notify the other party and it shall provide the other party with reasonable co-operation and assistance in relation to any such complaint, notice or communication.

2.7 The Supplier shall indemnify us and keep us indemnified at its own expense against all claims, liabilities, damages, administrative fines, costs or expenses incurred by us or for which we may become liable due to any failure by the Supplier or its Sub-Processors, subcontractors, agents or personnel to comply with any of its obligations under this Schedule or under the Data Protection Laws.

3. **Law and jurisdiction**

3.1 This Agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and interpreted in accordance with the laws of England and Wales.

3.2 The parties irrevocably agree that the courts of England and Wales have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) that arise out of, or in connection with, this Agreement or its subject matter or formation.