Data Processor Procedure

‘Working Together to expect the best’

Managing Suppliers & Third-Party Data

Last updated: March 2022
Review Date: March 2023
Version: 1
Document owner:

The Federation of Savile Town CE (C) Infant & Nursery School and Thornhill Lees CE (VC) Infant & Nursery School

Introduction

This process applies to all external suppliers, subcontractors and third parties (herein referred to as 'suppliers') that process data on behalf of The Federation of Savile Town CE (C) Infant & Nursery School and Thornhill Lees CE (VC) Infant & Nursery School**.** This policy details the procedure the school will follow throughout the process of managing those suppliers the school will work with from selection through to completion.

Responsibilities

The Business Manager in conjunction with the Finance Department and Data Protection Officer (DPO) are responsible for approving the selection of suppliers that process personal data on behalf of the school.

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

The IT Manager / Department is responsible for ensuring that adequate technical and other resources are available to support and manage the relationship between the school and said suppliers.

The Business Manager is responsible for carrying out regular audits of supplier compliance.

Procedure

Any supplier that process personal data on behalf of the school will only be selected if they can provide the technical, physical and organisational security required by the school.

Any suppliers outside of the United Kingdom will only be selected if they meet the same high levels of data compliance set out in the UK General Data Protection Regulations and associated Data Protection Act, 1998.

If the Business Manager and / or Data Protection Officer consider it necessary, a data security risk assessment will be carried out in the form of a questionnaire (Annex A). This will be dependent on the nature of the personal data being processed or the circumstances of the processing.

Where it is not possible to complete a questionnaire, further compliance checks will be made on the supplier to assess compliance; the Business Manager and DPO will then make a decision on whether to engage.

In most cases, the school will require a written agreement and confirmation of appropriate security measures from the supplier regarding the processing of personal data prior to partaking in any services. An example data sharing agreement from the Information Commissioners Office (ICO) is provided at Annex B should the school need to draft an agreement.

Any data processing agreement with the supplier will allow the school to conduct regular audits of the security arrangements during the period(s) in which the supplier has access to personal information.

Suppliers will need to request written authorisation from the school if they intend to outsource any part of the data processing service they provide. Any contracts with second-level suppliers or subcontractors will only be approved if they agree to comply with at least the same security and provisions of the primary organisation.

When a supplier contract / agreement is terminated, any personal data held by them, and any subcontractors will be securely destroyed or returned to the school.

A register of all suppliers who process personal data will be retained for school records along with any completed data sharing agreements, questionnaires and related documentation.

In addition to the register, a copy of all supplier privacy notices will be retained on the school system to identify how they intend to process and personal data from the school.

ANNEX A

DRAFT LETTER AND INFORMATION SECURITY QUESTIONNAIRE FOR SUPPLIERS, CONTRACTORS AND THIRD PARTIES

[Insert Supplier Name and Address]

Date:

Dear Sir/Madam,

UK-GDPR Compliance

As a school we are continually working towards ensuring compliance with the UK GDPR and Data Protection Act.

As a supplier, sub-contractor or third-party utilising school data, you need to confirm that you have undertaken a necessary review of your processes and procedures to ensure compliance with the relevant data protection laws. To continue with our commercial relationship, we need written confirmation that the current contract or arrangements will be agreeable and reflect the school's compliance standards.

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

We require the enclosed form to be completed, signed and returned to the School Business Manager either using the electronic system or by post. We reserve the right to request any additional information from you about your processes and procedures that will enable us secure compliance with the UK-GDPR requirements.

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

Thank you for your assistance.

Kind regards

[insert school name], School Business Manager

School name: [insert school name]

To comply with our compliance arrangements, please ensure that your Company:

Supplier Requirement	**Confirm consent and process**
Only uses the data we provide or that you access from our organisation in accordance with our instructions.	
Ensure that all parties in your organisation understand that any data they have access to or use which relates to our students or staff is confidential and must not be shared with anyone without our prior agreement.	
Take all steps to keep our 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 subcontract 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 with the transfer of any data.	
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? Please enclose any relevant procedures.	
That you will delete or return (at our choice) all personal data at the end of the agreement (unless storage is required by your current member state law)	
You will make available to the us all information necessary to demonstrate compliance; allow/contribute to audits (including inspections if necessary)	
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 organisations strategy for achieving compliance with the UK-GDPR?	
Please provide details of your Data Protection/Information Security/Cyber Security Policy as appropriate.	

I, [insert name] on behalf of [insert company name] confirm that the responses above are accurate and conform to the commercial agreement between [insert school name] and [insert company name].

Signed…….

Dated……..

Role within organisation……..

ANNEX B

ICO TEMPLATE DATA SHARING AGREEMENT FOR USE WITH SUPPLIERS AND OTHER THIRD PARTIES.

This Data Processing Agreement ("Agreement") forms part of the Contract for Services ("Principal Agreement") between _____

(the "**Company**")

and _____

(the "**Data Processor**")

(together as the "**Parties**")

WHEREAS

(A) The Company acts as a Data Controller.

(B) The Company wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor.

(C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (UK) GDPR & Data Protection Act 2018.

(D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. **Definitions and Interpretation**

1.1 Unless otherwise defined herein, capitalised terms and expressions used in this Agreement shall have the following meaning:

1.1.1 "**Agreement**" means this Data Processing Agreement and all Schedules;

1.1.2 "**Company Personal Data"** means any Personal Data Processed by a Contracted Processor on behalf of Company pursuant to or in connection with the Principal Agreement;

1.1.3 "**Contracted Processor**" means a Subprocessor;

1.1.4 "**Data Protection Laws**" means UK Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.5 "**UK**" means the United Kingdom; ;

1.1.7 "**UK-GDPR**" means UK General Data Protection Regulation;

1.1.8 "**Data Transfer**" means:

1.1.8.1 a transfer of Company Personal Data from the Company to a Contracted Processor; or

1.1.8.2 an onward transfer of Company Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.9 "**Services**" means the IT support services the Company provides.

1.1.10 "**Subprocessor**" means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Company in connection with the Agreement.

1.2 The terms, "**Commission", "Controller", "Data Subject", "Member State", "Personal Data",** "**Personal Data Breach", "Processing" and "Supervisory Authority**" shall have the same meaning as in the UK-GDPR, and their cognate terms shall be construed accordingly.

2**. Processing of Company Personal Data**

2.1 Processor shall**:**

2.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

2.1.2 not Process Company Personal Data other than on the relevant Company's documented instructions.

2.2 The Company instructs Processor to process Company Personal Data.

3. **Processor Personnel**

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. **Security**

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. **Subprocessing**

5.1 Processor shall not appoint (or disclose any Company Personal Data to) any Subprocessor unless required or authorised by the Company.

6. **Data Subject Rights**

6.1 Taking into account the nature of the Processing, Processor shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

6.2.1 promptly notify Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

6.2.2 ensure that it does not respond to that request except on the documented instructions of Company or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws Data Processing Agreement — Your Company inform Company of that legal requirement before the Contracted Processor responds to the request.

7. **Personal Data Breach**

7.1 Processor shall notify Company without undue delay upon Processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Processor shall co-operate with the Company and take reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. **Data Protection Impact Assessment and Prior Consultation**

Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required by article 35 or 36 of the UK-GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. **Deletion or return of Company Personal Data**

9.1 Subject to this section 9 Processor shall promptly and in any event within 10 business days of the date of cessation of any Services involving the Processing of Company Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Company Personal Data.

9.2 Processor shall provide written certification to Company that it has fully complied with this section 9 within 10 business days of the Cessation Date.

10. **Audit rights**

10.1 Subject to this section 10, Processor shall make available to the Company on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Company or an auditor mandated by the Company in relation to the Processing of the Company Personal Data by the Contracted Processors.

10.2 Information and audit rights of the Company only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. **Data Transfer**

11.1 The Processor may not transfer or authorise the transfer of Data to countries outside the UK without the prior written consent of the Company. If personal data processed under this Agreement is transferred from a country within the UK to a country outside the UK, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on approved standard contractual clauses for the transfer of personal data.

12. **General Terms**

12.1 **Confidentiality**. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("**Confidential Information**") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that: (a) disclosure is required by law; (b) the relevant information is already in the public domain.

12.2 Notices. All notices and communications given under this Agreement must be in writing

Specific Sharing Agreement
The Purpose of the agreed sharing of personal data and how this will be used?:
List the personal data that will be shared:

Signed:

Organisation (Data Controller)

Name

Position

Date

Organisation (Data Processor)

Name

Position

Date