

MANAGING SUB-CONTRACTED PROCESSING PROCEDURE

POLICY NUMBER & CATEGORY	QSC/12/APP7	Quality & Standards
VERSION NO & DATE	1	March 2018
ANTICIPATED REVIEW DATE:	March 2020	

CONTENTS

1	SCOPE	2
2	POLICY	2
3	PROCEDURE	2

1 SCOPE

1.1 All external suppliers that process personal data on behalf of Focus School Dunstable and Northampton Campus (hereafter the school) are within the scope of this procedure.

2 POLICY

2.1 The Data Protection Lead (DPL) with trust delegation, is 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 external data processing is contracted out in line with this procedure.

2.3 The FLT IT Department 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 FLT Data Protection Officer is responsible for carrying out regular audits of third-party compliance.

3 PROCEDURE

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

3.1.1 The FLT Legal & Compliance Department has in place appropriate checks that ensure all contracts are reviewed to see if personal data is processed. These checks are carried out even if data processing activities are not the primary reason for the contract.

3.1.2 The data controller (the school) will ensure that the all security arrangements are outlined in the contract with the external processor.

3.2 Suppliers from outside the EU (if none are available within the EU,) will only be selected under the following conditions, in addition to the conditions noted elsewhere in this procedure:

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

3.2.2 where there are legally binding corporate rules, and organisational and technical safeguards, established between the school and the supplier to secure the rights and freedoms of data subjects at least equal to those afforded within the EU; or

3.2.3 where the arrangement has been approved by the supervisory authority.

3.3 An information security risk assessment, taking into account the information security controls of ISO 27001 Annex A, is carried out before a supplier is engaged. Supplier risk assessments are conducted in line with the Risk Assessment Procedure.

3.4 If the DPL considers it necessary because of the nature of the personal data to be processed or because of the particular circumstances of the processing, an audit of the supplier's security arrangements against the requirements of ISO 27001 may be conducted before entering into the contract. Supplier audits are conducted in line with Managing Third Party Service Contracts.

3.5 The school requires a written agreement to provide the service as specified and requires the supplier to provide appropriate security for the personal data it will process.

- 3.6** All data processing contracts allow the school to conduct regular audits of the supplier's security arrangements during the period in which the supplier has access to the personal data.
- 3.7** All data processing contracts forbid suppliers from using further subcontractors without the school's written authorisation for the processing of personal data.
- 3.7.1** Where the school permits a supplier to subcontract processing of personal data, the immediate supplier must prohibit the second-level contractor (or further down the chain) from subcontracting these processing operations without the school's written authorisation.
- 3.8** 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 data will either be destroyed or returned to the school, and so on down the chain of sub-contracting.

