Schedule 1 Data Processing

The following additional terms shall apply to this Agreement and any:

Controller, Processor, Data Subject, Personal Data, Personal Data Breach, and Data Protection Officer: take the meaning given in the GDPR.

Data Protection Legislation:

(i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time
(ii) the DPA 2018 to the extent that it relates to processing of Personal Data and privacy;
(iii) all applicable Law about the processing of Personal Data and privacy;

Data Protection Impact Assessment: an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.

Data Loss Event: any event that results, or may result, in unauthorised access to Personal Data held by the Provider under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.

Data Subject Access Request: a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.

DPA 2018: Data Protection Act 2018

GDPR: the General Data Protection Regulation *(Regulation (EU) 2016/679)*

LED: Law Enforcement Directive *(Directive (EU) 2016/680)*

Protective Measures: appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it.

Staff: all persons employed by the Provider together with the Provider's servants, agents, Providers and Sub-Contractors used in the performance of its obligations under this Agreement.

Sub-processor: any third Party appointed to process Personal Data on behalf of the Provider related to this Agreement

1. DATA PROTECTION

1.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Council is the Controller and the Provider is the Processor. The only processing that the Provider is authorised to do is listed in this Schedule by the Council and may not be determined by the Provider.

1.2 The Provider shall notify the Council immediately if it considers that any of the Council's instructions infringe the Data Protection Legislation.

1.3 The Provider shall provide all reasonable assistance to the Council in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Council, include:

(i) a systematic description of the envisaged processing operations and the purpose of the processing;
(ii) an assessment of the necessity and proportionality of the processing operations in relation to the nature of this Agreement;
(iii) an assessment of the risks to the rights and freedoms of Data Subjects; and
(iv) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

1.4 The Provider shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

(i) process that Personal Data only in accordance with this Schedule, unless the Provider is required to do otherwise by Law. If it is so required the Provider shall promptly notify the Council before processing the Personal Data unless prohibited by Law;
(ii) ensure that it has in place Protective Measures, which have been reviewed and approved by the Council as appropriate to protect against a Data Loss Event having taken account of the:

(i) nature of the data to be protected;
(ii) harm that might result from a Data Loss Event;
(iii) state of technological development; and
(iv) cost of implementing any measures;

(iii) ensure that:

(i) the Staff do not process Personal Data except in accordance with this Agreement (and in particular this Schedule);
(ii) it takes all reasonable steps to ensure the reliability and integrity of any Staff who have access to the Personal Data and ensure that they:
(iii) are aware of and comply with the Provider's duties under this paragraph;
(iv) are subject to appropriate confidentiality undertakings with the Provider or any Sub-processor;
(v) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Council or as otherwise permitted by this Agreement; and (vi) have undergone adequate training in the use, care, protection and handling of Personal Data;

(iv) not transfer Personal Data outside of the EU unless the prior written consent of the Council has been obtained and the following conditions are fulfilled:

(i) the Council or the Provider has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Council;
(ii) the Data Subject has enforceable rights and effective legal remedies;
(iii) the Provider complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Council in meeting its obligations); and
(iv) the Provider complies with any reasonable instructions notified to it in advance by the Council with respect to the processing of the Personal Data;
(v) at the written direction of the Council, delete or return Personal Data (and any copies of it) to the Council on termination of the Agreement unless the Provider is required by Law to retain the Personal Data.

1.5 Subject to paragraph 1.6, the Provider shall notify the Council immediately if it:

(i) receives a Data Subject Access Request (or purported Data Subject Access Request);
(ii) receives a request to rectify, block or erase any Personal Data;
(iii) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(iv) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;
(v) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
(vi) becomes aware of a Data Loss Event.

1.6 The Provider's obligation to notify under paragraph 1.5 shall include the provision of further information to the Council in phases, as details become available.

1.7 Taking into account the nature of the processing, the Provider shall provide the Council with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 1.5 (and insofar as possible within the timescales reasonably required by the Council) including by promptly providing:

(i) the Council with full details and copies of the complaint, communication or request;
(ii) such assistance as is reasonably requested by the Council to enable the Council to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
(iii) the Council, at its request, with any Personal Data it holds in relation to a Data Subject;
(iv) assistance as requested by the Council following any Data Loss Event;
(v) assistance as requested by the Council with respect to any request from the Information Commissioner's Office, or any consultation by the Council with the Information Commissioner's Office.

1.8 The Provider shall maintain complete and accurate records and information to demonstrate its compliance with this paragraph. This requirement does not apply where the Provider employs fewer than 250 staff, unless:
(i) the Council determines that the processing is not occasional;
(ii) the Council determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and
(iii) the Council determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

ANNEX A - Schedule of Processing, Personal Data and Data Subjects

1. The Provider shall comply with any further written instructions with respect to processing by the Customer (NCC).

2. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Subject matter of the processing	• Providers (including private, voluntary & independent sector, childminders, schools/academies) • Children • Parents
Duration of the processing	• Providers/Schools required to enter any relevant child level data mentioned below onto secure Provider Portal or any other secure file transfer system such as Erica or S2S on a termly basis, for as long as the child requires funding at the setting. • PVI providers are required to reconfirm Early Years inclusion details, such as attendance and other relevant child level data mentioned below, on an ongoing basis for long as the child is in receipt of early years

	funding at the setting.
Nature and purposes of the processing	<u>Collection:</u> • Providers collect information direct from parents on a paper 'Parent Declaration Form'. • Schools and academies collect information direct from parents on their own school registration form and/or 'Parent Declaration Form', Early Years Pupil Premium voluntary registration form. • Information regarding all data subjects is collected via the Inclusion Funding claim form on a termly basis. The purpose is to confirm the child's attendance at the setting and the continuing need for Inclusion Funding. • Inclusion information is also collected via Application and Review forms which include data from all subject matter. The purpose is for information to be considered at Panel (these meet approximately every 6 weeks) to potentially allocate Inclusion funding to the child, or consider the child's progress and current level of funding, in the case of Reviews. • NCC extract data from the BI hub on a twice termly basis to determine which children are on a Child in Need plan (CIN), Child Protection Plan (CPP), Education Health and Care Plan (EHCP) or Looked After Child (LAC). • NCC extract postcode level data only from DWP 2yo lists and send to providers. <u>Purpose</u>: • The purpose of all processing mentioned above is for NCC to allocate various funding streams to providers and children and to monitor the progress of vulnerable children who are in funded places, on a termly basis, and to allow NCC to complete statutory returns to DFE. • For postcode level data mentioned above, the purpose is to allow providers in the local area of the postcode to leaflet drop to promote and encourage the take up of 2 year funded places. <u>Recording:</u> • Provider/School/Academy transcribes data collected and inputs onto secure Provider Portal by means of a termly headcount task, Better Start task or via Self Update module. • Schools/Academies transcribe data collected either onto secure Provider Portal by means of a termly headcount task (schools claiming for 30 hours or 2 year olds only) or by entering data into their own system such as Sims or Scholarpack. • Schools/Academies transcribe parent level detail for EYPP purposes onto a spreadsheet template. • Schools/Academies not using secure Provider Portal transmit data to us in Excel spreadsheets via secure file transfer system such as Erica or S2S. • NCC flag vulnerable children as CIN/CPP/LAC/EHCP and allocate funding. <u>Retrieval:</u> • Providers and schools using the Provider Portal can retrieve and download any data that has been previously submitted. If data is download using the functionality of the portal it must be kept securely on the provider's own computer by means of password protection. Any paper printouts that the provider produces from their data, must be kept secure e.g. in a locked drawer or cabinet. Passwords to downloaded documents must also be securely stored.

	Transmission: • Transmission of data by the provider/school occurs in the secure Provider Portal or other secure file transfer system such as Erica/S2S. • Providers must use a secure email address for the transmission of Inclusion Funding claim, application and review forms, DAF/EYPP/LAC/adoption evidence, or any emails containing personal information of subjects to the local authority. • Messages in the body of an email referring to data subjects should ideally only refer to the subject by initials of forename and surname plus date of birth, or anonymized by using any TYOF reference or 30 hours code reference. • Reports of vulnerable children are transmitted via the secure Provider Portal to providers to inform them of allocated funding to individual children. • Transmission of postcode data occurs in the secure Provider Portal, or by encrypted email (Cryptshare).
Type of Personal Data	• Provider: Name of setting, forename and surname of registered person, setting address & postcode (may include home address & postcode of childminders), telephone number, email address, Ofsted Reg/DFE number if applicable, opening hours, expected numbers of children, copy of Ofsted Certificate or other certificate/confirmation of registration (Independent schools), signature of registered person or manager. • Child: forename, surname, date of birth, gender, home address & postcode, home language, ethnicity, no. weekly hours attended and claimed at setting, Two Year Old Funding (TYOF) code (if relevant), 30 hours code (if relevant), LAC status evidence (if relevant), DAF claim evidence (if relevant), description of high level needs (Inclusion only). For Inclusion funding only, the following may be collected, but is not limited to: medical letters, photographs, SFSS reports, PDSS referral forms, EHCP plan or other relevant documents which support the application. • Parent: forename, surname, date of birth, home address & postcode, NI number, relationship to child, parental responsibility, email address and telephone number, latter two if given in an portal funding application i.e. TYOF.
Categories of Data Subject	• Providers including staff • Child • Parent • Financial • Professionals and agencies involved with the child (Inclusion funding only)
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	• Providers are recommended to securely retain 'Parent Declaration Forms' and all other supporting forms such as Inclusion, DAF evidence, for 6 years after end of funding period, or as required by funding body, as they constitute financial records. • Providers may be audited by NCC including scrutiny of Parent Declaration Forms. Forms and evidence should then be destroyed as confidential waste after the period of 6 years after funding period has ended.