

Schedule of Data Processing

PART 1 - DEFINITIONS

1 Definitions

In this Schedule, the following definitions apply:

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

Criminal Conviction Data: has the meaning given in UK GDPR Art 10 and the DPA 2018 section 10.

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

Data Protection Legislation: (i) the UK GDPR; (ii) the DPA; and (iii) all applicable Law about the processing of personal data and privacy.

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.

Law: any law, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Provider is bound to comply.

Losses: losses, liabilities, damages, costs and expenses (including legal fees on a solicitor/client basis) and disbursements and costs of investigation, litigation, settlement, judgment interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty or otherwise.

Personnel: all directors, officers, employees, agents, consultants and suppliers of a Party and/or any Sub-processor engaged by that Party in the performance of its obligations under this Agreement.

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 such measures adopted by it.

Shared Personal Data: the Personal Data and Special Categories of Personal Data and Criminal Offence Data to be shared between the Parties under this Agreement.

Special Categories of Personal Data: the categories of personal data referred to in the DPA 2018 and in the UK GDPR.

Sub-processor: any third party appointed to process Personal Data on behalf of a Processor related to this Agreement.

UK GDPR: has the meaning as set out in section 3(10) of the DPA 2018, supplemented by section 205(4) of the DPA 2018.

PART 2 – PRELIMINARY ISSUES

2 Protection of Personal Data

Indemnity

- 2.1 The Provider shall indemnify the Council against any and all Losses incurred by the Council due to breach by the Provider of Data Protection Legislation or this Schedule.

Status of the Controller

- 2.2 The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under this Agreement will determine the status of each Party under the Data Protection Legislation. The Parties shall act as:
- (a) Independent Controller (where each Party determines separately the purposes and means of processing Personal Data).

PART 3 – CONTROLLER-CONTROLLER RELATIONSHIP

3 Where the Parties are Independent Controllers of Personal Data

- 3.1 With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the joint control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their processing of such Personal Data as Controller.
- 3.2 Each Party shall process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.
- 3.3 Where a Party has provided Personal Data to the other Party in accordance with paragraph 3.1, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.
- 3.4 The Parties shall be responsible for their own compliance with Articles 13 and 14 of the UK GDPR in respect of the processing of Personal Data for the purposes of this Agreement.
- 3.5 The Parties shall only provide Personal Data to each other:
- (a) to the extent necessary to perform their respective obligations under this Agreement;
 - (a) in compliance with the Data Protection Legislation (including by ensuring all required fair processing information has been given to affected Data Subjects);
 - (b) where the provision of Personal Data from one Party to another involves transfer of such data to outside the UK, if the prior written consent of the non-transferring Party has been obtained and the following conditions are fulfilled:
 - (i) the destination country has been recognised as adequate by the UK government in accordance with Article 45 of the UK GDPR or DPA 2018 section 74A; or
 - (i) the transferring Party has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the UK GDPR or DPA 2018 section 75) as determined by the non-transferring Party;
as well as any additional measures determined by the Controller being implemented by the importing party;
 - (ii) the Data Subject has enforceable rights and effective legal remedies;
 - (iii) the transferring Party 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 non-transferring Party in meeting its obligations); and
 - (iv) the transferring Party complies with any reasonable instructions notified to it in

advance by the non-transferring Party with respect to the processing of the Personal Data; and

(c) where it has recorded it in Annex C.

- 3.6 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, each Party shall, with respect to its processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.
- 3.7 A Party processing Personal Data for the purposes of this Agreement shall maintain a record of its processing activities in accordance with Article 30 of the UK GDPR and shall make the record available to the other Party upon reasonable request.
- 3.8 Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to this Agreement (**Request Recipient**):
- (a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or
 - (b) where the request or correspondence is directed to the other Party and/or relates to the other Party's processing of the Personal Data, the Request Recipient will:
 - (i) promptly, and in any event within 5 Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and
 - (ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by the Data Protection Legislation.
- 3.9 Each Party shall promptly notify the other Party upon it becoming aware of any Data Loss Event relating to Personal Data provided by the other Party pursuant to this Agreement and shall:
- (a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Data Breach;
 - (b) implement any measures necessary to restore the security of any compromised Personal Data;
 - (c) work with the other Party to make any required notifications to the Information Commissioner's Office or any other regulatory authority and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out there); and
 - (d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, except as required by Law.
- 3.10 Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under this Agreement as specified in Annex C.
- 3.11 Personal Data shall not be retained or processed for longer than is necessary to perform each Party's obligations under this Agreement which is specified in Annex C.
- 3.12 Where the Provider is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs 3.1 to 3.11.

ANNEX C – SHARING PERSONAL DATA BETWEEN INDEPENDENT CONTROLLERS

1. This Annex C shall be completed by the Council following agreement with the Provider.
1. The contact details of the Council's Data Protection Officer are DPO@nottsc.gov.uk.
2. The contact details of the Provider's Data Protection Officer are: **[insert Contact details]**
3. The Parties may update this Annex C at any time by written agreement signed by representatives of both Parties.

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 Access Module (PAM) or any other secure file transfer system such as S2S on a termly basis, for as long as the child requires funding at the setting. - Providers are required to reconfirm Early Years SEND 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 Provider Access Module or the Early Years SEND Funding process on a termly basis. The purpose is to confirm the child's attendance at the setting and the continuing need for Early Years SEND Funding if applicable. - EY SEND 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 to potentially allocate Early Years SEND 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). <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. <u>Recording:</u> - Provider/School/Academy transcribes data collected and inputs onto secure Provider Access Module by means of a termly headcount task, tracking progress task, sufficiency task or census collection form. This

	includes parental data and consent ticks to check eligibility codes, EYPP and Early Learning funding status for 2 year olds. • Schools/Academies transcribe data collected either onto secure Provider Access Module by means of a termly headcount task, tracking progress task or sufficiency task. • NCC flag vulnerable children as CIN/CPP/LAC/EHCP and allocate funding. <u>Retrieval:</u> • Providers and schools using the Provider Access Module 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. <u>Transmission:</u> • Transmission of data by the provider/school occurs in the secure Provider Access Module. • Providers must use a secure email address and/or <u>Cryptshare</u> for the transmission of Early Years SEND Funding claim, application and review forms, DAF/EYPP/LAC/adoption evidence, or any emails containing personal information of subjects to the local authority. Online application and review forms are available for Early Years SEND Funding on the <u>Provider web page</u>. • 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 2yr reference or extended hours code reference. • Supplementary funding payments for vulnerable children are held within the adjustments tab of each term in the secure Provider Access Module to enable providers to see funding allocated to individual children.
Type of Personal Data	• <u>Provider:</u> Name of setting, forename and surname of registered person, setting address (may include home address 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. • <u>Child:</u> forename, surname, date of birth, gender, home address, home language, ethnicity, no. weekly hours attended and claimed at setting, Early Learning for 2 year olds code (if relevant), extended entitlement hours code (if relevant), LAC status evidence (if relevant), DAF claim evidence (if relevant), description of high level needs (EY SEND only). For Early Years SEND 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. • <u>Parent:</u> forename, surname, date of birth, home address, NI number, relationship to child, parental responsibility, email address and telephone number, latter two if given in an online funding application

	i.e. 2 year old funding or working families expanded entitlement funding.
Categories of Data Subject	• Providers including staff • Child • Parent • Financial • Professionals and agencies involved with the child (Early Years SEND 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 EY SEND, 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. • It is recommended that forms and evidence should then be destroyed as confidential waste after the period of 6 years after funding period has ended.