Department for Education

Accreditation Agreement for privileged early access to Performance data

Between The Secretary of State for Education

and

FFT Education Ltd

Dated: 15 May 2017

THIS DEED is made on ~~16th~~ 31st **May 2017**.

BETWEEN:

(1) **The Secretary of State for Education** (the "**Data Controller**") of Sanctuary Buildings, Great Smith Street London SW1P 3BT ("**DfE**")

(2) **FFT Education Ltd** (the "**Receiving Organisation**") of 1st Floor, 79 Eastgate, Cowbridge, Vale of Glamorgan, CF71 7AA.

together "**the Parties**".

1. Introduction and Scope

1.1 DfE is responsible for the collation and management of the data used for school and college performance. For the purposes of this accreditation agreement (the "**Agreement**"), DfE is the Data Controller of the Performance Data.

1.2 This Agreement documents the mechanism by which Performance Data as set out, in Schedule 1, will be provided by the Data Controller to the Receiving Organisation and the obligations each must meet in the handling of the Performance Data. This Agreement also covers any Performance Data already held by the Receiving Organisation, as set out in Schedule 1.

1.3 This Agreement contains the entire understanding and agreement of the parties and sets out the terms and conditions under which personal data held by the Data Controller for the purposes of administering the Performance Data will be supplied to the Receiving Organisation. This Agreement also sets out the details of Performance Data, versions and estimated timings of data access and justification for the provision and retention of Performance Data including identifiable and sensitive data items.

1.4 This Agreement is also entered into for the purpose of ensuring compliance with the Data Protection Act 1998 and that the processing of personal data complies with the provisions of this Act.

1.5 This Agreement may not be amended except in writing and signed by authorised representatives of both DfE and the Receiving Organisation in accordance with Clause 13.

1.6 The ongoing requirement for data and the content of this Agreement will be reviewed at least annually in accordance with DfE's instructions.

2. Definitions

2.1 In this Agreement, the following terms shall have the following meanings:

Agreement	means this Accreditation Agreement for privileged early access to school and college Performance Data from the Analyse School Performance Service (ASP) by the Receiving Organisation, signed by the Receiving Organisation by way of acceptance of this Agreement.
Analyse School Performance (ASP) Service	means the service, which replaces RAISEonline from 21 April 2017.
Commencement Date	means the commencement date of this Agreement, as specified in Schedule 1.
Commissioner	means the Information Commissioner as defined in the Freedom of Information Act 2000.
Data Controller	DfE is the Data Controller in respect of the Performance Data.
Data Protection Legislation	means the Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection and Privacy Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (21 2003/2426) and all other applicable laws and regulations relating to processing of personal data and privacy in effect in any relevant territory from time to time, including where applicable the guidance and codes of practice issued by the Information Commissioner and any EU regulations not in existence at the time this Agreement was executed.
End Users	means schools, local authorities, diocesan and religious groups, Academy Trusts, National Society and Catholic Education users, and Ofsted Inspectors; and any other users authorised by the DfE from time to time, to whom the Receiving Organisation supplies products and services developed using the Performance Data, pursuant to the Permitted Use and the terms of this Agreement.
Initial Term	means the initial period of 12 months from the Commencement Date, as specified in clause 3.1 of this Agreement.
Insolvency Event	means the following: (a) A winding up petition is presented or an application is made for the appointment of a

provisional liquidator or an administrator or a receiver, or a notice of intention to appoint an administrator is filed at court, or a provisional liquidator or an administrator or an administrative receiver or a receiver, is appointed, or a scheme of arrangement or a voluntary arrangement is proposed, or any moratorium comes into effect; or

(b) A shareholders' meeting is convened for the purpose of considering a resolution to wind up (except for a members' voluntary liquidation exclusively for the purposes of a bona fide solvent reconstruction or amalgamation and where the resulting entity agrees to be bound by, or assumes, the obligations of such insolvent party under this Agreement) a resolution to wind up is passed or a winding up order is made; or

(c) A party to this Agreement is unable to pay its debts as they fall due within the meaning of section 123 of the Insolvency Act 1986; or

(d) An encumbrancer takes possession of, or a receiver, administrative receiver or similar officer is appointed over, the whole or any part of either party's business or assets or any other similar process in any relevant jurisdiction which has a similar or analogous effect.

Intellectual Property Rights means copyrights and related rights, design rights, database rights, patents, rights to inventions, know-how or trade secrets (whether patentable or not), trade and domain and business names, logos and devices, trade and service marks, moral rights or similar intellectual property rights (whether registered or unregistered and wherever in the world enforceable) together with any extensions, revivals or renewals thereof, and all pending applications therefore and rights to apply for any of the foregoing in each case as may now or in the future exist anywhere in the world.

Losses means any and all losses, liabilities, costs, claims, proceedings, actions, judgments, damages and expenses including (without limitation) any awards and/or penalties or fines imposed by any regulator including the Information Commissioner to the extent recoverable at law (and any associated costs thereto) and any legal and other professional fees, consultancy fees and expenses on a full indemnity basis.

NPD Personal Sensitive Data has the meaning as defined in Section 3 of the NPD User Guide at: https://www.gov.uk/government/publications/national-

	pupil-database-user-guide-and-supporting-information.
Performance Data	means any information contained within, or aggregated from (e.g. aggregations to school, college, LA, national), the Performance Data as defined in Schedule 1.
Permitted Use	means the purposes specified by the Data Controller for which the Receiving Organisation and any Permitted User are authorised to use the Performance Data as set out in Schedule 1.
Permitted User	means a person listed in Schedule 1 who has been authorised by the Data Controller to have access to the Performance Data to process it for the Permitted Use.
Receiving Organisation	means the person or organisation to whom it has been agreed to supply the Performance Data under this Agreement, as specified in the Schedule 1.
Renewal Period	means each 12 month period after the Initial Term as described in clause 3.1 of the Agreement.
Schedule	means the schedules of this Agreement.
Security Incident	means an actual, suspected or threatened unauthorised exposure, access, disclosure, use, communication, deletion, revision, encryption, reproduction or transmission of any component of Performance Data or unauthorised access or attempted access or apparent attempted access (physical or otherwise) to any Performance Data or any systems on which such Performance Data is processed or stored.
Termination Date	means the date when this Agreement is terminated in accordance with Clause 15.
Working Day	means a day (other than a Saturday or Sunday) on which banks are open for general business in the City of London.

2.2 The terms "data controller", "data processor", "data subject" "personal data", "process", "processing" and "sensitive personal data" shall have the meanings set out in the Data Protection Act 1998.

2.3 Clause, Schedule and paragraph headings shall not affect the interpretation of this Agreement.

2.4 A person includes a natural person, corporate or unincorporated body (whether or not having separate legal personality).

2.5 The Schedule forms part of this Agreement and shall have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Schedule.

2.6 Unless the context otherwise requires, words in the singular shall include the plural and in the plural shall include the singular.

2.7 Unless the context otherwise requires, a reference to one gender shall include a reference to the other gender.

2.8 A reference to a statute or statutory provision is a reference to it as amended, extended or re-enacted from time to time.

2.9 A reference to a statute or statutory provision shall include all subordinate legislation made from time to time under that statute or statutory provision.

2.10 References to clauses and Schedules are to the clauses and Schedules of this Agreement and references to paragraphs are to paragraphs of the relevant Schedule.

2.11 Any words following the terms "including"," include"," in particular" or "for example" or any similar phrase shall be construed as illustrative and shall not limit the generality of the related general words.

2.12 In the case of conflict or ambiguity between any provision contained in the body of this Agreement and any provision contained in the Schedule, the provision in the Schedule to this Agreement shall take precedence.

2.13 If the Data Controller is replaced by a successor body or have their relevant powers and responsibilities transferred to another body, then references to them in this Agreement shall be taken to apply to their successors until such time as this Agreement can conveniently be updated to reflect the change.

3. Duration

3.1 The Agreement shall commence with effect from the Commencement Date and subject to termination in accordance with Clause 15, shall continue for an initial period of 12 months ("Initial Term"). and at the end of the Initial Term it will be renewed automatically for successive periods of 12 months (each 12 month period being a "Renewal Period").

4. Data Controller

4.1 DfE is the Data Controller.

5. Licence

5.1 In consideration of the Receiving Organisation agreeing to comply with its obligations under this Agreement, the Data Controller grants to the Receiving Organisation a non-exclusive, non-transferable licence to receive and use the Performance Data strictly for the Permitted Use specified in Schedule One up to the Termination Date.

5.2 In the event that the Receiving Organisation wishes to use the Performance Data for any purpose which is not specified in the Permitted Use, the Receiving Organisation shall submit a request for a new use of the Performance Data for the Data Controller's consideration and approval.

6. Provision of Performance Data

6.1 The Data Controller agrees to provide the Receiving Organisation with access to the relevant Performance Data required for the Permitted Use as specified in Annex B to the Agreement.

6.2 The Data Controller will provide access to the Performance Data for the Receiving Organisation as set out in Schedule 1 of this Agreement. The Data Controller will not be liable for any delay in the supply of the Performance Data, however caused.

6.3 Receiving Organisations will access Performance Data using a designated secure login to the ASP service and the Receiving Organisation shall restrict such access to Permitted Users, keep login details confidential and ensure access is subject to the Data Controller's departmental security standards as detailed in Schedule 3.

7. Processing and Use of Performance Data

7.1 The Receiving Organisation will use the Performance Data solely for the Permitted Use, as specified in the Schedule 1, and will not retain or process the data for any other purposes. This Agreement will apply only when data is being supplied by the Data Controller to the Receiving Organisation for these purposes.

7.2 The Receiving Organisation shall ensure that the Performance Data is held securely and in strict confidence, that appropriate technical and organisational information security and processing procedures are established and maintained to ensure that all Performance Data provided in accordance with this Agreement are sufficiently protected against any unlawful or unauthorised processing. In ensuring the security of the Performance Data, the Receiving Organisation will restrict access to the Performance Data to the Permitted Users for the Permitted Use, as specified in the Schedule 1. Permitted Users having access to the Performance Data are specified in the Schedule 1, including sub-contractors

7.3A The Data Controller will consider the Receiving Organisation's proposed Permitted Users on a case by case basis. The Receiving Organisation shall ensure and confirm to the Data Controller that each proposed Permitted User:

7.3.1 has undergone satisfactory Baseline Personnel Security Standards (BPSS) clearance sufficient to demonstrate their suitability for access to the Performance Data;

7.3.2 is fully aware of and abides by the terms and conditions imposed under this Agreement and submits a signed Individual Declaration Form to the Data Controller for permission to use the Performance Data;

7.3.3 receives appropriate training regarding data protection and security to enable the Receiving Organisation to comply with principle 7 of the Data Protection Act and is accredited to international standard for information security (ISO27001).

7.3B The Receiving Organisation will keep an up-to-date audit log of all other End Users who have access to the Performance Data, and ensure these Users have confirmed they comply with Data Protection Legislation.

7.4 The Receiving Organisation shall not be entitled to assign or otherwise transfer its rights or obligations under this Agreement, in whole or part to any third party, without the prior written consent of the Data Controller.

7.5 The Performance Data shall not at any time be copied, broadcast or disseminated to any other third parties except in accordance with this Agreement or under instruction of the Data Controller.

7.6 The Receiving Organisation shall ensure that:

7.6.1 any Permitted Users processing the Performance Data shall be based in the UK;

7.6.2 the Receiving Organisation's systems for processing data and providing web-based access to schools and other organisations as covered under the Permitted Use, shall be securely hosted in the UK in a data centre which is accredited to ISO27001;

7.6.3 End Users of products and services developed by the Receiving Organisation pursuant to the Permitted Use are authorised, have the right to view the Performance Data, can only access pupil-level data for their own organisation and have confirmed acceptance of the terms of use including obligations to comply with Data Protection Legislation;

7.6.4 it complies with the government's Cyber Essential Scheme as detailed in Schedule 2;

7.6.5 it complies with the Data Controller's departmental security standards as detailed in Schedule 3.

7.7 The Parties to this Agreement shall comply with the provisions of the Data Protection Legislation so far as such provisions apply to processing carried out under this Agreement and the Receiving Organisation shall procure that its Permitted Users observe the provisions of the Data Protection Legislation.

7.8 The Receiving Organisation shall not use the Performance Data (unless permitted in Schedule 1) to identify individuals or to inform a decision to be made about any individual without the prior written approval of the Data Controller. The Performance Data may not be reproduced by the Receiving Organisation in a form that would allow a third party to identify or derive information about individuals who are the data subjects without the prior written approval of the Data Controller.

7.9 No steps will be taken to contact any party identified in the data unless under the instruction or authorisation of the Data Controller.

7.10 The Receiving Organisation shall fully co-operate with the Data Controller to ensure compliance with the Data Protection Legislation in respect of the Performance Data. The Receiving Organisation shall notify the Data Controller upon receiving, and shall assist the Data Controller, in complying with and responding to:

7.10.1 requests for subject access from data subjects;

7.10.2 an information notice, or any other notice (including in particular any de-registration, enforcement or transfer prohibition notice) served by the Information Commissioner;

7.10.3 complaints from data subjects; or

7.10.4 any investigation of any breach or alleged breach of the Data Protection legislation which relate to the Performance Data.

7.11 The Receiving Organisation shall promptly report to the Data Controller any circumstance which they become aware of which:

7.11.1 may mean that Clause 7.2 has not been complied with;

7.11.2 may cause any party to breach the Data Protection Legislation as a result of processing carried out in connection with this Agreement; or

7.11.3 may mean that there has been unauthorised processing of any personal data derived from the Performance Data which is the subject of this Agreement.

7.12 Each party shall promptly report to the other parties if it becomes aware of any Security Incident affecting the Performance Data processed under this Agreement.

7.13 Without prejudice to any other rights or remedies which the Data Controller may have, the Receiving Organisation acknowledges and agrees that damages would not be an adequate remedy for any breach by the Receiving Organisation and/or the Permitted Users of the provisions of this Agreement and the Data Controller shall be entitled to the remedies of injunction, specific performance and other equitable relief for any threatened or actual breach of any provision of this Agreement by the Receiving Organisation and/or the Permitted Users.

7.14 The Receiving Organisation shall be able to link the Performance Data to any data from the National Pupil Database ("NPD Data") which the Data Controller has approved for use by the Receiving Organisation for the Permitted Use (examples in Schedule 1).

7.15 Where the Receiving Organisation wishes to link Performance Data to any other data (bar exclusions already agreed and noted in Schedule 1) they hold then they must seek prior approval of the Data Controller. The Receiving Organisation must show the relevant conditions for processing of the Data Protection Legislation in that Performance Data shall be processed fairly and lawfully and, in particular that:

7.15.1 at least one of the conditions in Schedule 2 of the Data Protection Act 1998 is met; and

7.15.2 in the case of sensitive personal data (ethnicity, language or special education needs) at least one of the conditions of Schedule 3 of the Data Protection Act 1998 is also met.

8. Not Used

9. Review and Audit

9.1 The Data Controller reserves the right to carry out a full review on the anniversary of the Commencement Date of this Agreement, as specified in paragraph 2 of Schedule 1, but on reasonable notice, periodic checks may also be conducted by an authorised employee of the Data Controller to review security and/or confirm compliance of the Receiving Organisation with this Agreement and may result in requesting access to their premises for this purpose. Failure to provide sufficient guarantees in respect of

adequate security measures will be likely to result in the termination of the contract, and the Receiving Organisation will no longer receive the data detailed in the Schedule.

9.2 The Data Controller and their agents shall be entitled to audit the Receiving Organisation's compliance with its responsibilities under this Agreement in respect of technical and organisational security measures. This may include physical inspection and copying of records. The Receiving Organisation and its permitted users shall co-operate fully in allowing the Data Controller and its agents' access to premises, documents and equipment.

9.3 The Receiving Organisation must inform the Data Controller of any incidents that breach the terms of this Agreement. Where the Receiving Organisation is found to be in breach of any of the terms of this Agreement, including any supplementary terms set out in the schedule, this may result in termination of access to the data. This termination may be enacted by the Data Controller at any point during the year.

10. Warranties and indemnities

10.1 No warranty is given by the Data Controller as to the quality or accuracy of the Performance Data.

10.2 The Receiving Organisation warrants and undertakes to the Data Controller that at all material times it will comply with the provisions of the Data Protection Legislation so far as such provisions apply to it in respect of this Agreement and more particularly that it will not make or permit or pursue any analyses which allow the identification of individuals (unless permitted by the Schedule 1).

10.3 Each party warrants and undertakes that it has the capacity and full legal authority to enter into this Agreement, this Agreement has been executed by its duly authorised representative, the making of this Agreement does not conflict with any of its existing obligations and once signed this Agreement shall constitute its legal, valid and binding obligations

10.4 The Receiving Organisation shall indemnify the Data Controller for any losses arising as a result of:

10.4.1 the Receiving Organisation breaching the Data Protection Legislation;

10.4.2 the Receiving Organisation causing the Data Controller to be in breach of any of the Data Protection Legislation;

10.4.3 the Receiving Organisation breaching this Agreement.

11. Receiving Organisation as data controller

11.1 The Receiving Organisation in making an application for early access to Performance Data has determined the purpose and manner in which the Performance Data shall be processed for the Permitted Use and therefore assumes all of the obligations of a data controller in common with the DfE upon receipt of the Performance Data.

11.2 Should it be the case that the party referred to as the Data Controller in this Agreement is found to be in breach of the Data Protection legislation as a result of the Receiving Organisation's use of the Performance Data, or should the Receiving Organisation's breach any of the terms of this Agreement, the Receiving Organisation shall indemnify the Data Controller for any losses.

11.3 Should the Data Controller become aware that the Receiving Organisation is in material breach of the Data Protection legislation for any processing of the Performance Data, the Data Controller may report any such breach to the Information Commissioner

12. Exclusion of liability

12.1 The Data Controller does not have any obligations to the Receiving Organisation, whether in contract, tort, breach of statutory duty or otherwise, beyond their obligations expressly set out in this Agreement.

12.2 The Data Controller shall not have any liability (however caused) for any loss of profit, business, contracts, revenues, increased costs or expenses or any indirect or consequential loss arising under this Agreement.

12.3 The Data Controller does not exclude or limit their liability to the Receiving Organisation for:

12.3.1 fraud or fraudulent misrepresentation;

12.3.2 death or personal injury caused by negligence;

12.3.3 a breach of any obligations implied by section 12 of the Sale of Goods Act 1979 or Section 2 of the Supply of Goods and Services Act 1982; or

12.3.4 any matter for which it would be unlawful for the parties to exclude liability.

13. Variations from Agreement

13.1 In the event that either party wishes to vary any term of this Agreement then that party will give notice in writing to the offices of the other party, explaining the effect of and reason for the proposed variation.

13.2 This Agreement may not be assigned or otherwise transferred in whole or in part by the Receiving Organisation without the prior written consent of the Data Controller.

13.3 As the Data Controller for the personal data covered by this Agreement, the Data Controller will have the final decision on any proposed variation to this Agreement.

13.4 No amendment or variation to this Agreement, or any revocation or extension of this Agreement, shall be effective unless it is made in writing and signed by the parties.

14. Disputes

14.1 If any dispute arises in connection with this Agreement, senior representatives of each party with authority to settle the dispute will, within 10 Working Days of a written request from one party to the others, meet in a good faith effort to resolve the dispute.

14.2 If the dispute is not resolved at that meeting, the parties will attempt to settle it by mediation in accordance with the Centre for Effective Dispute Resolution (CEDR) Model Mediation Procedure. Unless otherwise agreed between the parties, the mediator will be nominated by CEDR. To initiate the mediation a party must give notice in writing ("ADR notice") to the other parties to the dispute requesting mediation. A copy of the request should be sent to CEDR Solve. The mediation will start not later than 20 Working Days after the date of the ADR notice.

14.3 No party may commence any court proceedings in relation to any dispute arising out of this Agreement until it has attempted to settle the dispute by mediation and either the mediation has terminated or one of the other parties has failed to participate in the mediation, provided that the right to issue proceedings is not prejudiced by a delay.

14.4 Nothing in this clause shall prevent any party seeking a preliminary injunction or other judicial relief at any time, if in its judgement such action is necessary to prevent irreparable damage.

14.5 This Agreement shall be governed by and construed in accordance with English Law and, to the extent disputes arising out of or relating to this Agreement are not settled under the above procedures, the Receiving Organisation submits to the exclusive jurisdiction of the English Courts.

15. Termination

15.1 In the event that either party wishes to exit from this Agreement, that party shall serve a notice by e-mail to the named primary and secondary contacts of the other party (as set out in the Schedule 1) of a date not less than 30 days from the date of the said notice on which the party proposes to exit this Agreement.

15.2 The Data Controller may without liability terminate this Agreement immediately by written notice to the Receiving Organisation if:

15.2.1 the Receiving Organisation commits a material breach of this Agreement and, if in the reasonable opinion of the Data Controller, this has not been properly remedied within 7 days of written notice of the breach being given on behalf of the Data Controller;

15.2.2 an Insolvency Event occurs in relation to the Receiving Organisation;

15.2.3 the Receiving Organisation is acting or has acted in a manner materially prejudicial to the Data Controller's goodwill and reputation.

15.3 The Receiving Organisation may without liability terminate this Agreement immediately by written notice to the Data Controller if:

15.3.1 the Data Controller commits a material breach of this Agreement and, if in the reasonable opinion of the Receiving Organisation, this has not been properly remedied within 7 days of written notice of the breach being given on behalf of the Receiving Organisation; or

15.3.2 the Receiving Organisation no longer requires the Performance Data for the Permitted Use.

15.4 The Receiving Organisation undertakes to destroy, within 20 Working Days of the expiry of this Agreement or the Termination Date, all copies of the Performance Data and expunge it from any computer, word processor or other device or medium containing it (including all documents, material or copies of such documents or materials embodying any of such Performance Data). Any information derived from the Performance Data produced for the Permitted Use which does not include any Personal Data, Sensitive Personal Data or NPD Sensitive Personal Data, which would enable the data subjects of the Performance Data to be identified, and which uses the Standard Disclosure Controls or an agreed alternative to prevent such identification may be retained. The Receiving Organisation will provide the Data Controller with a written assurance that the Performance Data has been destroyed within 20 Working Days of the Termination Date.

16. Consequences of termination

16.1 Termination of this Agreement, for any reason, shall not affect the accrued rights, remedies, obligations or liabilities of the parties existing at termination.

16.2 The following clauses shall survive the termination of this Agreement:

16.2.1 Definitions

16.2.2 Clause 3 - Duration

16.2.3 Clause 4 - Data Controller

16.2.4 Clause 7 - Processing and Use of Performance Data

16.2.5 Clause 8 - Publication / Reproduction of the Performance Data

16.2.6 Clause 10 - Warranties and Indemnities

16.2.7 Clause 11 - Receiving Organisation as Data Controller

16.2.8 Clause 12 - Exclusion of Liability

16.2.9 Clause 14 - Disputes

16.2.10 Clause 15 - Termination

16.2.11 Clause 16 - Consequences of Termination

16.2.12 Clause 17 - Freedom of Information Requests

16.2.13 Clause 19 - Intellectual Property Rights – Performance Data

17. Freedom of information requests

17.1 The Receiving Organisation acknowledges that the Data Controller is subject to the requirements of the Freedom of Information Act 2000 and the Environmental Information Regulations 2004 and agrees to provide all necessary assistance as required by the Data Controller to enable them to comply with their obligations under this legislation.

18. Publication of details of Agreement

18.1 The Receiving Organisation consents to the Data Controller publishing the following details on its website:

18.1.1 name of the Receiving Organisation;

18.1.2 a summary of the aims of the project or research being carried out;

18.1.3 tier of data requested;

18.1.4 whether or not it is a linked data request;

18.1.5 details of the outcome of the application.

18.2 For the avoidance of doubt, no personal data will be published by the Data Controller.

19. Intellectual property rights – Performance Data

19.1 All Intellectual Property Rights in the Performance Data and in any database containing the Performance Data compiled by the Data Controller are vested and shall remain vested in the Data Controller. The Receiving Organisation acknowledges that the Performance Data is derived from databases compiled and owned by the Data Controller and that the Data Controller retains all rights in the Performance Data and such databases under the Copyright Rights in Databases Regulations 1997.

20. Privileged early access to official statistics

20.1 Early access to Performance Data and statistics, in advance of the official publication date by the department, is being provided to the Receiving Organisation under the provisions set out in the Pre Release to Official Statistics Order 2008 and conditions imposed by the Data Controller as defined in this Agreement. The Receiving Organisation must abide by the rules set out in the 2008 Order, including that:

- any person who receives pre-release access must not disclose any statistic until after the official statistic has been published;
- any person who receives pre-release access must not use that access for personal gain until after the official statistic has been published or to take any action (other than the preparation of responses or statements as referred to in paragraph 3(1)(a)(i) of the 2008 Order) for political advantage; and
- that access must not be used to change or compromise the content, presentation or timing of publication of official statistics.

20.2 Performance Data and statistics must not be disclosed publicly or be shared with the institutions covered within the Permitted Use during the pre-release period before official statistics have been published. Restricted statistics that are provided in advance of the official publication date for the Permitted Use must not be made available to any institutions, nor released into the public domain in advance of the official publication date. No other local or national aggregate statistics may be disclosed publically or shared with institutions in advance of the official publication date. During the period before the official publication date the Receiving Organisation shall ensure that the Performance Data and statistics are only accessed by the Permitted Users who are identified in the Schedule 1 as having access to the pre-release data.

20.3 If the Receiving Organisation is found to be in breach of any of the conditions set out in the Pre Release Order and/or conditions defined in this Agreement, including the condition that if the Data Controller is no longer content that the public benefit of providing early access outweighs the detriment to public trust in official statistics likely to result from such access, this is considered as a breach and as such, this may result in termination of access to the data.

Schedule 1

1. Contact Details

1.1 Receiving Organisation Contact details

Receiving Organisation Name	**FFT Education Ltd**
Primary contact Name	[redacted]
Position	[redacted]
Telephone Number	[redacted]
e-mail Address	[redacted]

Secondary contact Name	[redacted]
Position	[redacted]
Telephone Number	[redacted]
e-mail Address	[redacted]

1.2 Data Controller Contact details

Approver of Dataset Releases – Primary Contact

Name	[redacted]
Position	[redacted]
Telephone Number	[redacted]
e-mail Address	[redacted]

Secondary Contact

Name	[redacted]
Position	[redacted]
Telephone Number	[redacted]
e-mail Address	[redacted]

2. Commencement Date of Accreditation Agreement

Commencement Date	31 May 2017

3. Performance Data available to Receiving Organisation

High Level Data Specification

3.1 List of the files that will be available upon achieving accreditation:

- EYFSP files (2016)
- School context (2016)
- QLA (2016)
- Phonics final (2016)
- KS1 final files (2016)
- KS2 validated files (2016)
- KS4 validated files (2016)
- 16-18 performance table amended files (2016) (SPT files only – no further breakdowns provided)

3.2. Description of Files

3.2.1 16-18 performance tables files, including national and school/college level aggregates for:

a. A level, academic, applied general and tech level students:

Progress: Value added score with confidence limits (or completion and attainment score for Tech levels)
Attainment: average point score per entry, average point score per entry expressed as a grade
Retention: % of students retained to the end of their main course of study

b. English and maths students (covering students that didn't achieve a good pass during key stage 4)
English: Average progress in English
Maths: Average progress in Maths

Pupil level and exam level files will also be provided

3.2.2 KS4 files, including national and school level aggregates for:

a. Progress8 and Attainment8 data and by subject area breakdowns
b. Achieving the English Baccalaureate and by subject breakdowns
c. English Baccalaureate subject area value added scores
   % Achieving A*-C in English and Maths
d. Average number of qualifications entered and points achieved
e. Subject entries and attainment
f. Relative performance indicators by subject

Most of the above files will also include the following pupil group breakdowns:

- Gender
- Disadvantaged
- Free School Meals
- Special Educational Needs
- English as a first Language
- Prior Attainment (Overall and by English and Maths)
- Ethnic group

Pupil level and exam level files will also be provided

3.2.3 KS2 files, including national and school level aggregates for:

a. % achieving the expected standard in reading, writing and maths combined
b. % achieving the higher standard in reading, writing and maths combined
c. Progress scores for each of reading, writing and maths
d. % achieving a scaled score of above 100 for each of reading, maths and EGPS
e. % achieving the high scaled score for each of reading, maths and EGPS
f. Average scaled score for each of reading, maths and EGPS
g. Average spelling mark and by mark bands
h. % achieving the expected standard for each of science and writing
i. % achieving the higher standard for writing

All of the above will include also include the following pupil group breakdowns:

- Gender
- Disadvantaged
- Free School Meals
- Special Educational Needs
- English as a first Language
- Prior Attainment (Overall and by English and Maths)
- Ethnic group

Pupil level and exam level files will also be provided

3.2.4 KS1 files, including national and school level aggregates for:

a. % achieving the expected standard in reading, writing, maths and science
b. % achieving the higher standard in reading, writing and maths
c. % below pre-KS1 level in reading, writing and maths
d. % at foundations level in reading, writing and maths
e. % working towards the level in reading, writing and maths

All of the above will include also include the following pupil group breakdowns:

- Gender
- Disadvantaged
- Free School Meals
- Special Educational Needs
- English as a first Language

- Prior Attainment by EYFS
- Ethnic group

Pupil level files will also be provided.

3.2.5 Phonics files, including national aggregates for:

a. % achieving the expected standard at the end of year 1
b. % achieving the expected standard at the end of year 2

All of the above will include also include the following pupil group breakdowns:

- Gender
- Free School Meals
- Special Educational Needs
- English as a first Language
- Ethnic group

Pupil level files will also be provided

3.2.6 EYFS file, including national and school level aggregates for:

a. % of pupils achieving a good level of development
b. % of pupils achieving at least the expected standard in the following:
   i. Communication and language
   ii. Literacy
   iii. Mathematics
   iv. Physical development
   v. Personal, social and emotional development
   vi. Understanding the world
   vii. Expressive arts and design

All of the above will include also include the following pupil group breakdowns:

- Gender
- Free School Meals

3.2.7 QLA files (with Programme of Study files), **including national aggregates for:**
a. Each question in each of the following KS2 papers:

   i. Reading
   ii. EGPS
   iii. Spelling
   iv. 3 Maths papers

All of the above will include also include the following pupil group breakdowns:

- Gender

Item level files will also be provided

3.2.8 Absence, including national aggregates for:

a. % of sessions missed
b. % of persistent absentees

All of the above will include also include the following pupil group breakdowns:

- Gender
- Free School Meals
- Special Educational Needs
- English as an first Language
- Ethnic group

3.2.9 Exclusions, including national aggregates for:

a. % of fixed term exclusions
b. % of pupils with 1 or more fixed term exclusions
c. % of pupils with more than 1 fixed term exclusion
d. % of permanent exclusions

All of the above will include also include the following pupil group breakdowns:

- Gender
- Free School Meals
- Special Educational Needs
- English as an first Language
- Ethnic group

3.2.10 Destinations, including national aggregates for:

a. % going to a sustained education or employment / training destination
b. % going to sustained education, and further breakdowns
c. % going to sustained employment and / or training
d. % not sustained in education or employment

All of the above will include also include the following pupil group breakdowns:

- Gender
- Disadvantaged

3.3 The timeline for release of data files can be found at Annex A to the Agreement.

4. Legislation applicable to the Performance Data

Legal Gateway under which Performance Data is being shared
Data Protection Act 1998
Education (School Performance Information) (England) Regulations 2015
Education (Individual Pupil Information) (Prescribed Persons) (England) Regulations 2009
Education (Student Information) (England) Regulations 2015
Education Act 1996
Freedom of Information Act 2000

5. Use of the Performance Data by the Receiving Organisation ("the Permitted Use")

5.1 The Receiving Organisation is permitted to use the Performance Data strictly for the development and delivery of products and services to End Users in compliance with the terms and conditions of this Agreement.

5.2 For the avoidance of doubt, the Permitted Use **does not include rights** to:

5.2.1 use the Performance Data to produce any analyses that do not support the objectives of the ASP service;

5.2.2 transmit, supply or deliver any products or services containing, or based on, Performance Data except via appropriate, role-based secure login access to persons with statutory rights or other verified permissions to access the Performance Data;

5.2.3 sell, share, publish or otherwise transmit the Performance Data in the public domain.

6. Permitted User(s) of Performance Data

Annex B lists the users which have access to the Performance Data to process it for the Permitted Use (as shown at 5 above). Any changes (additions, removals or name changes) will be made when the Agreement is reviewed but the necessary steps will be carried out by Receiving Organisation to remove access when a member of staff leaves the organisation, including sub-contractors.

Annex A

Supplier Data Requests & Release of Performance Data Timeline

NB. 2017 Data Release Dates will be provided later

	2016 Data files (Tick data files required)	2017 Data files (Tick data files required)	Tick if you require the selected files to be anonymised	2016 Data Release Date (earliest date)
16-18 performance table unamended files	✓	✓		Day after the Agreement Commencement date
16-18 performance table amended files	✓	✓		as above
16-18 performance table final files	✓	✓		as above
KS4 unamended files	✓	✓		as above
KS4 amended files	✓	✓		as above
KS4 final files	✓	✓		as above
KS2 unamended files	✓	✓		as above
KS2 amended files	✓	✓		as above
KS2 final files	✓	✓		as above
KS1 provisional files	✓	✓		as above
KS1 final files	✓	✓		as above
Phonics files	✓	✓		as above
Early years foundation profile files	✓	✓		as above
QLA files (including PoS files)	✓	✓		as above
Absence files	✓	✓		as above
Exclusions files	✓	✓		as above
Destinations	✓	✓		as above
School characteristics	✓	✓		as above

Table 1 - Identifying and Sensitive Data items

The table below provides details of identifying and/or sensitive data (including highly sensitive data), together with any corresponding mappings, where applicable. There will be circumstances where access to some or all of this data is required to undertake some research or analysis. Only the Tier 1 and Tier 2 data items listed below will be included in the data files, where applicable.

Tier 1 data items	Tier 2 data Items
Unique Pupil Numbers (UPN)	
Unique Learner Numbers (ULN)	
Names	
Postcode	
Date of birth / age within academic year	Age and month part of age of pupil at the start of the academic year. Year and month of birth
Ethnicity (extended ethnic codes)	Ethnic group (20 main group codes)
Primary and secondary special educational need (SEN) type	SEN provision
Pupil Premium indicator	
	Free school meals (FSM) eligibility, including Ever FSM indicators
	Pupil mobility indicator
	Persistent absentee indicator

Please sign here:

Signature: [redacted]

Signed by (print name): [redacted]

Company name: FFT Education Ltd.

Date: 30th May 2017

Date received by DfE: 31 May 2017

Department for Education

Revised 25 May 2017

Annex B – List of Permitted Users

NOTE - Permitted Users who require access to Performance Data during the period before official statistics are published by DfE must be identified, type '**YES**' in the '**Early access to Data required**' column.

All Permitted Users including **sub-contractors must be listed in the table below, including:** company name and address, company number, individual name, job title, and reason for access to data and indicate if they will require early access to data.

Company Name, Address and Company Number	Individual Name	Job Title	Reason for access to data	Early access to Data required (Yes / No)
FFT Education Ltd. Unit 7, 27 Milton Park, Abingdon, Oxfordshire , OX14 4SA No: 3685684	[redacted]	[redacted]	Data processing	Yes
			Data processing	Yes
			Data processing	Yes
			Data processing	Yes
			Data processing	Yes
			Data processing	Yes
			Data processing	Yes
			Data processing	Yes
			Data processing	Yes
			Data processing	Yes
			Data processing	Yes
			Data processing & analysis	Yes
			Data processing & analysis	Yes
			DBA (Privileged User)	Yes
			IT Support (Privileged User)	Yes
			IT Support (Privileged User)	Yes
			Monitoring access	Yes
			Monitoring access (SIRO)	Yes
			QA & support	Yes
			QA & support	Yes
			QA & support	Yes
			QA & support	Yes
			QA & support	Yes
			QA & support	Yes
			QA & support	Yes
			QA & support	Yes
			QA & support	Yes
			QA & support	Yes
			QA & support	Yes
			QA & support	Yes
			QA & support	Yes

Company Name, Address and Company Number	Individual Name	Job Title	Reason for access to data	Early access to Data required (Yes / No)
FFT Education Ltd. Unit 7, 27 Milton Park, Abingdon, Oxfordshire , OX14 4SA No: 3685684	[redacted]	[redacted]	Supporting school & LA users	
			Supporting school & LA users	
			Supporting school & LA users	
			Supporting school & LA users	Not know
			Supporting school & LA users	to follow
			Supporting school & LA users	
			Supporting school & LA users	
			Supporting school & LA users	
			Supporting school & LA users	
			Supporting school & LA users	
			Supporting school & LA users	
			Supporting school & LA users	
			Supporting school & LA users	
			Supporting school & LA users	
			Supporting school & LA users	
			Supporting school & LA users	
			Supporting school & LA users	
			Supporting school & LA users	
			Supporting school & LA users	
			Supporting school & LA users	
			Supporting school & LA users	
			Supporting school & LA users	
			Supporting school & LA users	
			Supporting school & LA users	
			Training schools & LAs	
			Training schools & LAs	
			Training schools & LAs	
			Training schools & LAs	
			Training schools & LAs	
			Training schools & LAs	
			Data Analysis and Research	
			Data Analysis and Research	
			Data Analysis and Research	
			Data Analysis and Research	
			Data Analysis and Research	
			Data Analysis and Research	

65

Schedule 2

Cyber Essentials Scheme

Cyber Essentials is a government-backed, industry supported scheme to help organisations protect themselves against common cyber attacks. The Cyber Essentials Requirements document sets out the necessary technical controls. The Assurance Framework shows how the independent assurance process works and the different levels of assessment organisations can apply for to achieve the badges. It also contains guidance for security professionals carrying out the assessments.


Cyber_Essentials...


bis-15-72-cyber...

Schedule 3

Data Controller (DfE) Security Standards

For contracts, which require the holding or processing of either personal data and/or OFFICIAL data, the successful Receiving Organisations will need to assure the DfE that they can comply with the Department's security standards.

Definitions

NB. CESG's function as National Technical Authority has been subsumed into the new National Cyber Security Centre (NCSC). NCSC have assumed responsibility for publication of cyber security policy and guidance which can be found on the NCSC website at https://www.ncsc.gov.uk/guidance.

"BPSS" "Baseline Personnel Security Standard"	a level of security clearance described as pre-employment checks in the National Vetting Policy.
"CESG" "Communications Electronics Security Group" *NB. Reference to NCSC at the beginning of Schedule 3.*	is the UK government's National Technical Authority for Information Assurance.
"CESG IAP" "CESG Information Assurance Policy Portfolio" *NB. Reference to NCSC at the beginning of Schedule 3.*	means the CESG Information Assurance policy Portfolio containing HMG policy and guidance on the application of 'security assurance' for HMG systems. – see above note re NCSC.
"CTAS" "CESG Tailored Assurance" *NB. Reference to NCSC at the beginning of Schedule 3.*	is an 'information assurance scheme' which provides assurance for a wide range of HMG, MOD, Critical National Infrastructure (CNI) and public sector customers procuring IT systems, products and services, ranging from simple software components to national infrastructure networks.

"CPA" "CESG Product Assurance" *NB. Reference to NCSC at the beginning of Schedule 3.*	is an 'information assurance scheme' which evaluates commercial off the shelf (COTS) products and their developers against published security and development standards. These CPA certified products can be used by government, the wider public sector and industry.
"CCSC" "CESG Certified Cyber Security Consultancy" *NB. Reference to NCSC at the beginning of Schedule 3.*	is CESG's approach to assessing the services provided by consultancies and confirming that they meet CESG's standards. This approach builds on the strength of CLAS and certifies the competence of suppliers to deliver a wide and complex range of cyber security consultancy services to both the public and private sectors.
"CCP" "CESG Certified Professional" *NB. Reference to NCSC at the beginning of Schedule 3.*	is a CESG scheme in consultation with government, industry and academia to address the growing need for specialists in the cyber security profession and are building a community of recognised professionals in both the UK public and private sectors.
"CC" "Common Criteria"	the Common Criteria scheme provides assurance that a developer's claims about the security features of their product are valid and have been independently tested against recognised criteria.
"Cyber Essentials" "Cyber Essentials Plus"	Cyber Essentials is the government backed, industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme.
"Data" "Data Controller" "Data Processor"	shall have the meanings given to those terms by the Data Protection Act 1998

"Personal Data" "Sensitive Personal Data" "Data Subject", "Process" and "Processing"	
"Department's Data" "Department's Information"	is any data or information owned or retained in order to meet departmental business objectives and tasks, including: (a) any data, text, drawings, diagrams, images or sounds (together with any repository or database made up of any of these components) which are embodied in any electronic, magnetic, optical or tangible media, and which are: (i) supplied to the Receiving Organisation by or on behalf of the Department; or (ii) which the Receiving Organisation is required to generate, process, store or transmit pursuant to this Contract; or (b) any Personal Data for which the Department is the Data Controller;
"DfE" "Department"	means the Department for Education
"Departmental Security Standards"	means the Department's security policy or any standards, procedures, process or specification for security that the Receiving Organisation is required to deliver.
"Digital Marketplace / GCloud"	the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects. Cloud services (e.g. web hosting or IT health checks) are on the G-Cloud framework.

"FIPS 140-2"	this is the Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), entitled 'Security Requirements for Cryptographic Modules'. This document is the de facto security standard used for the accreditation of cryptographic modules.
"Good Industry Practice" "Industry Good Practice"	means the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.
"Good Industry Standard" "Industry Good Standard"	means the implementation of products and solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.
"GSC" "GSCP"	means the Government Security Classification Policy which establishes the rules for classifying HMG information. The policy is available at: https://www.gov.uk/government/publications/government-security-classifications
"HMG"	means Her Majesty's Government
"SPF" "HMG Security Policy Framework"	This is the definitive HMG Security Policy which describes the expectations of the Cabinet Secretary and Government's Official Committee on Security on how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely.
"ICT"	means Information and communications technology (ICT) is used as an extended synonym for information technology (IT), used to describe the bringing together of enabling technologies used to deliver the end-to-end solution

IS5	this is HMG Information Assurance Standard No. 5 - Secure Sanitisation issued by CESG
"ISO/IEC 27001" "ISO 27001"	is the International Standard for Information Security Management Systems Requirements
"ISO/IEC 27002" "ISO 27002"	is the International Standard describing the Code of Practice for Information Security Controls.
"ISO 22301"	is the International Standard describing for Business Continuity
"IT Security Health Check" "Penetration Testing"	means an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity or availability of information held on that IT system.
"Need-to-Know"	the Need-to-Know principle is employed within HMG to limit the distribution of classified information to those people with a clear 'need to know' in order to carry out their duties.
"OFFICIAL" "OFFICIAL-SENSITIVE"	the term 'OFFICIAL' is used to describe the baseline level of 'security classification' described within the Government Security Classification Policy (GSCP) which details the level of protection to be afforded to information by HMG, for all routine public sector business, operations and services. the 'OFFICIAL–SENSITIVE' caveat is used to identify a limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media, as described in the Government Security Classification Policy.
"Security and Information Risk Advisor" "CCP SIRA" "SIRA"	the Security and Information Risk Advisor (SIRA) is a role defined under the CESG CESG Certified Professional Scheme

1. The Receiving Organisation shall comply with the requirements under Cabinet Office Procurement Policy Note – Use of Cyber Essentials Scheme certification - Action Note 09/14 25 September 2014, or any subsequent updated document; that "contractors supplying products or services to HMG shall have achieved, and retain certification at the appropriate level, under the HMG Cyber Essentials Scheme".

2. The Receiving Organisation shall have achieved, and be able to maintain, independent certification to ISO/IEC 27001 (Information Security Management Systems Requirements). The scope of certification and the statement of applicability must be acceptable, following review, to DfE, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).

3. The Receiving Organisation shall follow the UK Government Security Classification Policy (GSCP) in respect of any Departmental Data being handled in the course of providing this service, and will handle this data in accordance with its security classification. (In the event where the Receiving Organisation has an existing Protective Marking Scheme then the Receiving Organisation may continue to use this but must map the HMG security classifications against it to ensure the correct controls are applied to the Departmental Data).

4. The Receiving Organisation shall segregate Departmental Data being handled from other data on the Receiving Organisation's own IT equipment to both protect the Departmental Data and enable it to be identified and securely deleted when required. In the event that it is not possible to segregate any Departmental Data then the Receiving Organisation shall be required to ensure that it is stored in such a way that it is possible to securely delete the data.

5. The Receiving Organisation shall have in place and maintain physical security and entry control mechanisms (e.g. door access) to premises and sensitive areas and separate logical access controls (e.g. identification and authentication) to ICT systems to ensure only authorised personnel have access to Departmental Data.

6. The Receiving Organisation shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Departmental Data, including but not limited to: physical security controls; good industry standard policies and process; anti-virus and firewalls; security updates and up-to-date patching regimes for anti-virus solutions; operating systems, network devices, and application software, user access controls and the creation and retention of audit logs of system use.

7. The Receiving Organisation must ensure any electronic transfer methods across public space or cyberspace, including third party provider networks must be protected via encryption which has been certified to a minimum of FIPS 140-2 standard or a similar method approved by the DfE prior to being used for the transfer of any Departmental Data.

8. Storage of Departmental Data on any portable devices or media shall be limited to the absolute minimum required to deliver the stated business requirement and shall be subject to Clauses 10 and 11 below.

9. Any portable removable media (including but not constrained to pen drives, flash drives, memory sticks, CDs, DVDs, or other devices) which handle, store or process Departmental Data to deliver and support the service, shall be under the control and

configuration management of the Receiving Organisation providing the service, shall be both necessary to deliver the service and shall be encrypted using a product which has been certified to a minimum of FIPS140-2 standard or use another encryption standard that is acceptable to DfE.

10. All portable ICT devices, including but not limited to laptops, tablets, smartphones or other devices, such as smart watches, which handle, store or process Departmental Data to deliver and support the service, shall be under the control and configuration management of the Receiving Organisation. These devices shall be full-disk encrypted using a product which has been certified to a minimum of FIPS140-2 standard or use another encryption standard that is acceptable to DfE.

11. Whilst in the Receiving Organisation's care all removable media and hardcopy paper documents containing Departmental Data must be handled securely and secured under lock and key when not in use and shall be securely destroyed when no longer required, using either a cross-cut shredder or a professional secure waste paper organisation.

12. When necessary to hand carry removable media and/or hardcopy paper documents containing Departmental Data, the media or documents being carried shall be kept under cover and transported in such a way as to ensure that no unauthorised person has access to the material being carried. This clause shall apply equally regardless of whether the material is being carried inside or outside of company premises.

13. Subject to clause 15.4 of this Agreement, at the end of the contract or in the event of equipment failure or obsolescence, all Departmental information and data, in either hardcopy or electronic format, that is physically held or logically stored on the Receiving Organisation's ICT infrastructure must be securely sanitised or destroyed in accordance with the current HMG policy (HMG IS5) using a CESG approved product or method. Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as a Storage Area Network (SAN) or shared backup tapes, then the Receiving Organisation shall protect the Department's information and data until the time, which may be long after the end of the contract, when it can be securely cleansed or destroyed.

14. Access by the Receiving Organisation to Departmental Data shall be confined to those individuals who have a "need-to-know" and the appropriate level of security clearance, as required by the Department for those individuals whose access is essential for the purpose of their duties. All employees with direct or indirect access to Departmental Data must be subject to pre-employment checks equivalent to or higher than the Baseline Personnel Security Standard (BPSS)

15. All Receiving Organisation employees who handle Departmental Data must have annual awareness training in protecting information.

16. The Receiving Organisation shall, as a minimum, have in place robust and ISO 22301 conformant Business Continuity arrangements and processes including IT disaster recovery plans and procedures to ensure that the delivery of the contract is not adversely affected in the event of an incident. An incident shall be defined as any situation that might be, or could lead to, a disruption, loss, emergency or crisis. When a certificate is not available it shall be necessary to verify the ongoing effectiveness of the ISO 22301 conformant Business Continuity arrangements and processes including IT disaster recovery plans and procedures, to the extent that the Receiving Organisation

must have tested/exercised these plans within the last 12 months and produced a written report of the test/exercise, outcome and feedback, including required actions.

17. Any non-compliance with these Departmental Security Standards, or other Security Standards pertaining to the solution, or any suspected or actual breach of the confidentiality, integrity or availability of Departmental Data being handled in the course of providing this service, shall be investigated immediately and escalated to the Department by a method agreed by both parties.

18. Receiving Organisations shall ensure that any IT systems and hosting environments that are used to hold Departmental Data being handled, stored or processed in the course of providing this service shall be subject to an independent IT Health Check (ITHC) using a CESG approved ITHC provider before access to data is given. The findings of the ITHC relevant to the service being provided are to be shared with the Department and all necessary remedial work carried out. In the event of significant security issues being identified, a follow up remediation test may be required.

19. The Receiving Organisation will provide the Department with full details of any actual storage outside of the UK or any future intention to host Departmental Data outside the UK or to perform any form of ICT management or support function from outside the UK. The Receiving Organisation will not go ahead with any such proposal without the prior written agreement from the Department.

20. The Department reserves the right to audit the Receiving Organisation providing the service within a mutually agreed timeframe but always within seven days of notice of a request to audit being given. The audit shall cover the overall scope of the service being supplied and the Receiving Organisation's compliance with the clauses contained in this Section.

21. The Receiving Organisation shall contractually enforce all these Departmental Security Standards onto any third-party suppliers, sub-contractors or partners who could potentially access Departmental Data.

22. The Receiving Organisation shall deliver ICT solutions and services that are compliant with the HMG Security Policy Framework in conjunction with current CESG Information Assurance Policy Portfolio and Departmental Policy. The Receiving Organisation will provide the Department with evidence of compliance for the solutions and services to be delivered. The Department's expectation is that the Receiving Organisation shall provide written evidence of:

    a. Existing security assurance for the services to be delivered, such as: PSN Compliance as a PSN Customer and/or as a PSN Service; CESG Tailored Assurance (CTAS); inclusion in the Common Criteria (CC) or CESG Product Assurance Schemes (CPA); ISO 27001 / 27002 or an equivalent industry level certification. Documented evidence of any existing security assurance or certification shall be required.

    b. Existing HMG security accreditations that are still valid including: details of the body awarding the accreditation; the scope of the accreditation; any caveats or restrictions to the accreditation; the date awarded, plus a copy of the residual risk statement. Documented evidence of any existing security accreditation shall be required.

    c. Documented progress in achieving any security assurance or accreditation

activities including whether documentation has been produced and submitted. The Receiving Organisation shall provide details of who the awarding body or organisation will be and date expected.

23. If no current security accreditation or assurance is held the Receiving Organisation and sub-contractors shall undergo appropriate security assurance activities as determined by the Department. Contractor and sub-contractors shall support the provision of appropriate evidence of assurance and the production of the necessary security documentation. This will include obtaining any necessary professional security resources required to support the Contractor's and sub-contractor's security assurance activities such as: a CESG Certified Cyber Security Consultancy (CCSC) or CESG Certified Professional (CCP) Security and Information Risk Advisor (SIRA)

Signatories

In signing below, the parties are agreeing to the terms and conditions set out in this Agreement.

This deed has been entered into and delivered on the date stated at the beginning of this Agreement.

Executed as a deed by affixing the common seal of the Secretary of State for Education in the presence of

The Corporate Seal of the Secretary

of State for Education hereunto affixed is

Authenticated by: [redacted]

(Duly authorised)

Date: 31/5/17

Executed as a deed by **FFT Education Ltd** acting by [redacted], a director, in the presence of:

[redacted]
[SIGNATURE OF WITNESS]

[redacted].....
[NAME OF WITNESS [IN BLOCK CAPITALS]]

[redacted].....
.....
.....
[ADDRESS OF WITNESS]

[redacted].....
[OCCUPATION OF WITNESS]

..[redacted]
[SIGNATURE OF DIRECTOR]
[redacted]

Date: 16th May 2017