DATA SHARING AND PROCESSING
TABLE OF CONTENTS:

<table>
<thead>
<tr>
<th>Item</th>
<th>Heading</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Data Processing Agreement</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>Data Protection Act 1998</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>Data Protection Act – Compliance</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>Data Requests &amp; Usage</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>Data Processing</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>Customer Data Transfer</td>
<td>5</td>
</tr>
<tr>
<td>7</td>
<td>Data Retention and Destruction</td>
<td>6</td>
</tr>
<tr>
<td>8</td>
<td>Additional Information</td>
<td>6</td>
</tr>
<tr>
<td>9</td>
<td>Law and Jurisdiction</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Appendix 1. Sensitive Personal Data</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Appendix 2. ISO 27001 Certificate</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Appendix 3. Data Protection Act Schedule 2</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Appendix 4. Data Protection Act Schedule 3</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Appendix 5. Data Protection Act Interpretation of the Principles</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>Appendix 6. Data Sharing Agreements</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>Appendix 7. Supplier Self-Certification Statements</td>
<td>17</td>
</tr>
</tbody>
</table>
1 DATA PROCESSING AGREEMENT

This document has been developed for Schools, Local Authorities and Customers of Capita Business Services Limited, trading as Capita Children’s Services (‘Capita’ and ‘CCS’ respectively) to ensure a full understanding of the processes and procedures undertaken by Capita in the treatment and processing of Customer Data as a Data Processor (as defined under the Data Protection Act 1998, the ‘Act’) on behalf of Data Controllers (as defined under the Act). The document is also intended to inform and confirm to the users of the Capita and CCS services the level of commitment undertaken by Capita and CCS to the safety and security of client data entrusted to them for processing.

2 DATA PROTECTION ACT 1998

As a business Capita (and CCS) are governed by and regulated under the Data Protection Act 1998 in relation to its dealings with all customer data and is obliged to operate in full compliance with the 8 Data Protection Principals set out under the Act.

Schedule 1 to the Act lists the Data Protection Principles in the following terms:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
   i) at least one of the conditions in Schedule 2 is met, and
   ii) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. About the rights of individuals e.g. personal data shall be processed in accordance with the rights of data subjects (individuals).
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

In order to achieve these objectives Capita and CCS operate at, or exceed, industry standard best practice in the treatment and processing of Customer Data across all geographic offices and the Bedford offices (main Data Processing site) have obtained ISO 27001 accreditation (Appendix 2) as confirmation of the high levels of control and security undertaken in the day to day operations which relate to dealing with all Customer Data. These Processes and Procedures are institution wide and are supported and enforced from board level down to all staff who are involved in dealing with Customer Data. Where deemed necessary, any office dealing with Customer Data as a Data Processor will be included in the formal ISO 27001 accreditation structure.

As defined under section 2 of the Act – see Appendix 1 for more details.
Operating processes and procedures are fully documented, maintained and, where relevant, audited by Capita Information Security and Compliance personnel (a central Capita Group department established in part to ensure data security across the whole Capita Group of companies). In this respect the Capita and CCS compliance teams requires the completion of an annual Information Security questionnaire, which relates to the ISO 27001 compliance from all offices dealing with Customer Data processing.

For Commercial and/or Security reasons specific details relating to locations of and security measures employed at the Capita Data Processing Centres will not be made generally available but Capita can confirm that these details have been inspected, reviewed and verified in the ISO 27001 verification processes. The Data Centre security processes and procedures are fully documented, maintained and, where relevant, audited by Capita Information Security and Compliance personnel.

3 DATA PROTECTION ACT – COMPLIANCE

Under the Act, personal and/or sensitive data can only be shared or disclosed by the Data Controller to the Data Processor if, in the case of personal data, at least 1 condition under Schedule 2 (see Appendix 3) is met, or in the case of personal sensitive data at least 1 condition under Schedule 3 (see Appendix 4) is met. It is the responsibility of the Data Controller to obtain requisite authorisation and to inform Data Subjects (as defined under the Act) by means of a privacy notice – formally a ‘fair processing notice’ (as defined in Schedule 1, Part II of the Act – see Appendix 5).

In accordance with the Act the Data Controller may disclose data to the Data Processor ‘for the performance of a contract’ and for ‘systematic data sharing’ for the purposes of records management. In the processing of Customer Data Capita and CCS will process the Data strictly in accordance with the instructions provide by the Data Controller and not further or otherwise.

Capita and CCS confirm that they have processes in place to ensure that all relevant employees are compliant with the UK Data Protection Act 1998 as amended, and with consideration to the Isle of Man Data Protection Act 2002 and Data Protection (Jersey) Law 2005.

Additionally, in line with principles 7 and 8, Capita and CCS place very strict controls around who has visibility of any Customer Data held on their servers. For the investigation and resolution of support incidents involving Customer Data, Capita and CCS may request permission for our offshore teams in India (or other countries without adequacy) to have remote access to the data, but only when anonymised data cannot be used to resolve the issue and under no circumstances is this data ever allowed to be physically transferred and is retained within the Capita Data Centres (all of which are located within the EEA). Access to the Customer Data in these circumstances is provided by a secure remote access solution.

Any such access must be approved in advance in writing by the Data Controller/Customer, whether on a per instance basis, or by a signed Data Processing/Sharing Agreement. Please refer to Appendix 6 for samples of the various documents including the European Commission approved ‘model’ clauses.
4 DATA REQUESTS & USAGE

In line with principles 3 and 6 of the Act, Capita and CCS will only request customer data where necessary. The primary purposes for such requests shall be:

i. The investigation and resolution of Support Incidents, including data fixes. This is on a single instance basis, with prior written approval.
ii. For pre-defined User Acceptance Testing (UAT).
iii. For Pilot testing and the testing of generic patches.
iv. For the creation of sanitised data.
v. Data Conversions for new customers.
vi. For the implementation of a Hosted Service for the Data Controller.

Capita and CCS maintain strict controls relating to data used outside of these environments and all staff members receive annual awareness training and are required to read and understand the Information Security Policies and Standards. Customer Data will not be processed in a Test Environment without prior customer approval.

The teams requiring Customer Data will be responsible for the security of the customer data whilst on the Capita/CCS network. Each item of Customer Data will be managed by a specific Capita/CCS Data Owner.

Capita/CCS acknowledges and accepts that it is processing the Data as a service provider and Data Processor and that the Data and all intellectual property rights in the Data shall belong to the Data Controller absolutely.

5 DATA PROCESSING

Capita and CCS as the Data Processor(s) undertake that they shall:

(i) Process the Data at all times in accordance with the Act and solely for the purposes (connected with provision by the Data Processor of the Services) and in the manner specified from time to time by the Data Controller in writing and for no other purpose or in any manner except with the express prior written consent of the Data Controller;

(ii) in a manner consistent with the Act and with any guidance issued by the Information Commissioner, implement appropriate technical and organisational measures to safeguard the Data from unauthorised or unlawful Processing or accidental loss, destruction or damage, and that having regard to the state of technological development and the cost of implementing any measures, such measures shall ensure a level of security appropriate to the harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage and to the nature of the Data to be protected;

(iii) ensure that each of its employees, agents and subcontractors are made aware of its obligations under this Agreement with regard to the security and protection of the Data and shall require that they enter into binding obligations with the Data Processor in order to maintain the levels of security and protection provided for in any agreement between the Data Controller and the Data Processor;
(iv) not divulge the Data whether directly or indirectly to any person, firm or company or otherwise without the express prior written consent of the Data Controller except to those of its employees, agents and subcontractors who are engaged in the Processing of the Data and are subject to the binding obligations referred to in clause (iii) or except as may be required by any law or regulation;

(v) in the event of the exercise by Data Subjects of any of their rights under the Act in relation to the Data, inform the Data Controller as soon as possible, and the Data Processor further agrees to assist the Data Controller with all data subject information requests which may be received from any Data Subject in relation to any Data;

(vi) not physically transfer Personal Data outside of the EEA except with the express prior written authority of the Data Controller; with respect to third-party processing, the Data Processor will retain the Data strictly within the EEA and will only permit secure remote access to named individuals from trusted organisations outside of the EEA.

6 CUSTOMER DATA TRANSFER

Transferring Data

With respect to transferring customer data there are two principle scenarios:

- Providing CCS staff with access to secure data storage environments.
- Physical transit of the data, whether internally or externally.

In both cases, the act of transferring this data will be documented or logged for auditing purposes. Customer data shall only be transferred from or to the recipient via one of the approved transit methods, which are:

- SFTP - either the CCS' solution, or a customer's own secure solution, with the data encrypted.
- LANdesk, via the use of Data Collection PCs
- By email, with the exception of full databases, to external recipients validated in CRM/MIS.

Data sent externally will always be encrypted. The use of this will be on a customer by customer basis, dependent on Data Processing Agreements and secure solutions available.

- A manual collection/delivery where a same day, point to point journey is possible, in line with the Capita Group Policy.
- Delivery/collection via a Capita Group approved same-day secure courier.
- Internal network transfer, or by granting access permission to the data internally - with the awareness of the Data Owner2.
- Physical transfer within a single CCS site by the use of an encrypted hard drive.

Where files are encrypted, this will be to an AES 256 level. Passwords or access codes will be sent via an alternative medium.

2 For the investigation and resolution of support incidents involving Customer Data, Capita and CCS will request prior written permission from the Data Controller for Capita offshore teams in India (or other countries without adequacy) to access data. In this event Capita and CCS will use unmodified European Commission approved model clauses in the documentation to approve the transfer by the Data Controller – see Appendix 6.
Customer Data will not be physically transferred to third parties, whether in the UK, or offshore without express prior written permission from the Data Controller.

7 DATA RETENTION AND DESTRUCTION

Data will be retained as follows:

- SFTP logins and folders will only be kept active for 30 days.
- Customer data files will be destroyed within 90 days of a Support Incident being closed.
- Customer data files will be destroyed within 180 days of the customer go-live for Data Conversion work. This is to allow for both school holidays and issues where corrections may be required.
- Information relating to Support Incidents is to be held within the Capita CCS CRM or MIS systems for 6 years+ current. This does not include screenshots, or data files.

No customer data will be backed up unless it is located in a Hosted Service environment. All data is stored and disposed of in line with the requirements of the Capita Group Information Security Asset Classification & Handling Standard.

Where Customer Data is held on equipment which has reached the end of its useful life it is Capita Policy to have the hard drive of such equipment securely destroyed rather than being overwritten to current CESG standards as defined at www.cesg.gov.uk.

8 ADDITIONAL INFORMATION

Where Customers use the Capita Cloud based Software Solutions for Schools, there is more information available at Appendix 7. This information is provided in response to a Department for Education project in conjunction with the Information Commissioners Office and major Educational Cloud providers to develop a resource for schools which will enable them to use the guidance to make informed decisions regarding their Personal and Sensitive Data and how they can safely comply with their responsibilities as Data Controllers under the Data Protection Act.

9 LAW AND JURISDICTION

All Capita and CCS Data Processing agreements are governed by and shall be construed in accordance with the Laws of England and Wales. Each party to a Capita/CCS agreement, which involves or requires Data Processing as an element of the agreement, shall be required to submit to the non-exclusive jurisdiction of the courts of England and Wales.
Appendix 1.

DATA PROTECTION ACT 1998

Section 2

SENSITIVE PERSONAL DATA
In this Act ‘sensitive personal data’ means personal data consisting of information as to—

(a) the racial or ethnic origin of the data subject,
(b) his political opinions,
(c) his religious beliefs or other beliefs of a similar nature,
(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
(e) his physical or mental health or condition,
(f) his sexual life,
(g) the commission or alleged commission by him of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.
ISO 270001 Certificate:

The management system of Capita Business Services Ltd
Priory Court, Cardington, Bedford, MK44 3JZ

has been assessed and certified as meeting the requirements of

ISO 27001:2013
for the following activities

Database design, development and support services

Further clarifications regarding the scope of this certificate and the applicability of requirements may be obtained by consulting the certifier.

Valid from 31 March 2015 until 30 March 2017

Authorised by

Chief Executive
The British Assessment Bureau
www.british-assessment.co.uk

Certification is conditional on maintaining the required performance standards throughout the certified period of registration
The British Assessment Bureau, 3D Tower View, Kings Hill, Kent, ME19 4DY
DATA PROTECTION ACT 1998

SCHEDULE 2 Part 1

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE:
PROCESSING OF ANY PERSONAL DATA

1 The data subject has given his consent to the processing.

2 The processing is necessary—
   (a) for the performance of a contract to which the data subject is a party, or
   (b) for the taking of steps at the request of the data subject with a view to entering into a contract.

3 The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4 The processing is necessary in order to protect the vital interests of the data subject.

5 The processing is necessary—
   (a) for the administration of justice,
       (i) for the exercise of any functions of either House of Parliament,
   (b) for the exercise of any functions conferred on any person by or under any enactment,
   (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
   (d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

6 (a) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.
   (b) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.
DATA PROTECTION ACT 1998

SCHEDULE 3

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE:
PROCESSING OF SENSITIVE PERSONAL DATA

1. The data subject has given his explicit consent to the processing of the personal data.

2. (a) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

   (b) The Secretary of State may by order—
      (i) exclude the application of sub-paragraph (a) in such cases as may be specified, or
      (ii) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3. The processing is necessary—
   (a) in order to protect the vital interests of the data subject or another person, in a case where—
      (i) consent cannot be given by or on behalf of the data subject, or
      (ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or
   (b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4. The processing—
   (a) is carried out in the course of its legitimate activities by any body or association which—
      (i) is not established or conducted for profit, and
      (ii) exists for political, philosophical, religious or trade-union purposes,
   (b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,
   (c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and
   (d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6. The processing—
   (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
   (b) is necessary for the purpose of obtaining legal advice, or
   (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
Appendix 4 (cont’d).

7 (a) The processing is necessary—
   (i) for the administration of justice, for the exercise of any functions of either House of Parliament,
   (ii) for the exercise of any functions conferred on any person by or under an enactment, or
   (iii) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.
(b) The Secretary of State may by order—
   (i) exclude the application of sub-paragraph (a) in such cases as may be specified, or
   (ii) provide that, in such cases as may be specified, the condition in sub-paragraph (a) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.
(c) The processing
   (1) is either—
      (i) the disclosure of sensitive personal data by a person as a member of an anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation; or
      (ii) any other processing by that person or another person of sensitive personal data so disclosed; and
   (2) is necessary for the purposes of preventing fraud or a particular kind of fraud.
(d) In this paragraph ‘an anti-fraud organisation’ means any unincorporated association, body corporate or other person which enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud or which has any of these functions as its purpose or one of its purposes.

8 (a) The processing is necessary for medical purposes and is undertaken by—
   (i) a health professional, or
   (ii) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.
(b) In this paragraph “medical purposes” includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9 (a) The processing—
   (i) is of sensitive personal data consisting of information as to racial or ethnic origin,
   (ii) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
   (iii) is carried out with appropriate safeguards for the rights and freedoms of data subjects.
(b) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (a)(i) and (ii) is, or is not, to be taken for the purposes of sub-paragraph (a)(iii) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10 The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.
Appendix 5.

SCHEDULE 1 Part II

INTERPRETATION OF THE PRINCIPLES IN PART I

The first principle

1 (a) In determining for the purposes of the first principle whether personal data are processed fairly, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed.

(b) Subject to paragraph 2, for the purposes of the first principle data are to be treated as obtained fairly if they consist of information obtained from a person who—
   (i) is authorised by or under any enactment to supply it, or
   (ii) is required to supply it by or under any enactment or by any convention or other instrument imposing an international obligation on the United Kingdom.

2 (a) Subject to paragraph 3, for the purposes of the first principle personal data are not to be treated as processed fairly unless—
   (i) in the case of data obtained from the data subject, the data controller ensures so far as practicable that the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph (3), and
   (ii) in any other case, the data controller ensures so far as practicable that, before the relevant time or as soon as practicable after that time, the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph (3).

(b) In sub-paragraph (1)(b) ‘the relevant time’ means—
   (1) the time when the data controller first processes the data, or
   (2) in a case where at that time disclosure to a third party within a reasonable period is envisaged—
      (i) if the data are in fact disclosed to such a person within that period, the time when the data are first disclosed,
      (ii) if within that period the data controller becomes, or ought to become, aware that the data are unlikely to be disclosed to such a person within that period, the time when the data controller does become, or ought to become, so aware, or
      (iii) in any other case, the end of that period.

(c) The information referred to in sub-paragraph (1) is as follows, namely—
   (i) the identity of the data controller,
   (ii) if he has nominated a representative for the purposes of this Act, the identity of that representative,
   (iii) the purpose or purposes for which the data are intended to be processed, and
   (iv) any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.

3 (a) Paragraph 2(a)(ii) does not apply where either of the primary conditions in sub-paragraph (b), together with such further conditions as may be prescribed by the Secretary of State by order, are met.
Appendix 5 (cont’d)

(b) The primary conditions referred to in sub-paragraph (a) are—
   (i) that the provision of that information would involve a disproportionate effort, or
   (ii) that the recording of the information to be contained in the data by, or the disclosure of the data by, the data controller is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4  (a) Personal data which contain a general identifier falling within a description prescribed by the Secretary of State by order are not to be treated as processed fairly and lawfully unless they are processed in compliance with any conditions so prescribed in relation to general identifiers of that description.

(b) In sub-paragraph (1) ‘a general identifier’ means any identifier (such as, for example, a number or code used for identification purposes) which—
   (i) relates to an individual, and
   (ii) forms part of a set of similar identifiers which is of general application.

The second principle

5 The purpose or purposes for which personal data are obtained may in particular be specified—
   (i) in a notice given for the purposes of paragraph 2 by the data controller to the data subject, or
   (ii) in a notification given to the Commissioner under Part III of this Act.

6 In determining whether any disclosure of personal data is compatible with the purpose or purposes for which the data were obtained, regard is to be had to the purpose or purposes for which the personal data are intended to be processed by any person to whom they are disclosed.

The fourth principle

7 The fourth principle is not to be regarded as being contravened by reason of any inaccuracy in personal data which accurately record information obtained by the data controller from the data subject or a third party in a case where—
   (i) having regard to the purpose or purposes for which the data were obtained and further processed, the data controller has taken reasonable steps to ensure the accuracy of the data, and
   (ii) if the data subject has notified the data controller of the data subject’s view that the data are inaccurate, the data indicate that fact.

The sixth principle

8 A person is to be regarded as contravening the sixth principle if, but only if—
   (i) he contravenes section 7 by failing to supply information in accordance with that section,
   (ii) he contravenes section 10 by failing to comply with a notice given under subsection (1) of that section to the extent that the notice is justified or by failing to give a notice under subsection (3) of that section,
   (iii) he contravenes section 11 by failing to comply with a notice given under subsection (1) of that section, or
The seventh principle

9 Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to—
   (i) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and
   (ii) the nature of the data to be protected.

10 The data controller must take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.

11 Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle—
   (i) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and
   (ii) take reasonable steps to ensure compliance with those measures.

12 Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless—
   (a) the processing is carried out under a contract—
      (i) which is made or evidenced in writing, and
      (ii) under which the data processor is to act only on instructions from the data controller, and
   (b) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.

The eighth principle

13 An adequate level of protection is one which is adequate in all the circumstances of the case, having regard in particular to—
   (i) the nature of the personal data,
   (ii) the country or territory of origin of the information contained in the data,
   (iii) the country or territory of final destination of that information,
   (iv) the purposes for which and period during which the data are intended to be processed,
   (v) the law in force in the country or territory in question,
   (vi) the international obligations of that country or territory,
   (vii) any relevant codes of conduct or other rules which are enforceable in that country or territory (whether generally or by arrangement in particular cases), and
Appendix 5 (cont’d)

(viii) any security measures taken in respect of the data in that country or territory.

14 The eighth principle does not apply to a transfer falling within any paragraph of Schedule 4, except in such circumstances and to such extent as the Secretary of State may by order provide.

15 (a) Where—

(i) in any proceedings under this Act any question arises as to whether the requirement of the eighth principle as to an adequate level of protection is met in relation to the transfer of any personal data to a country or territory outside the European Economic Area, and

(ii) a Community finding has been made in relation to transfers of the kind in question, that question is to be determined in accordance with that finding.

(b) In sub-paragraph (1) ‘Community finding’ means a finding of the European Commission, under the procedure provided for in Article 31(2) of the Data Protection Directive, that a country or territory outside the European Economic Area does, or does not, ensure an adequate level of protection within the meaning of Article 25(2) of the Directive.
Appendix 6.

Included below are examples of Data Sharing Agreements including the Data Processing Annual Agreement which is constructed to comprise the unaltered European Commission model clauses.

<table>
<thead>
<tr>
<th>No.</th>
<th>File - Document</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Data Processing Annual Agreement - v1-3.pdf</td>
<td>Data Processing Annual Agreement comprising the unaltered European Commission model clauses</td>
</tr>
<tr>
<td>2</td>
<td>DATA Agreement of Use Form - Development &amp; Testing.pdf</td>
<td>Data Processing Agreement – using data provided by a customer for software development work</td>
</tr>
<tr>
<td>3</td>
<td>DATA Agreement of Use Form - Hosted SIMS.pdf</td>
<td>Data Processing Agreement - using data provided by a customer to assist the Hosted SIMS support team for the purpose of troubleshooting and supporting the schools use of the hosted service.</td>
</tr>
<tr>
<td>4</td>
<td>DATA Agreement of Use Form - User Testing.pdf</td>
<td>Data Processing Agreement - using data provided by a customer to members of the CCS User Acceptance test team only, for internal User Acceptance Testing.</td>
</tr>
<tr>
<td>5</td>
<td>DATA Agreement of Use Form -ONE Customers.pdf</td>
<td>Data Processing Agreement - using data provided by a customer for Case investigation purposes and for System (Integration) and acceptance Testing purposes for ONE.</td>
</tr>
</tbody>
</table>
Appendix 7.

CLOUD SOFTWARE SERVICES FOR SCHOOLS
Supplier self-certification statements with service and support commitments

Click on the icon below to review the document.