Data Protection Assurance Statement

Organisation Name:	D L Solutions
Data Protection Officer Name:	Danny Lagden
Address:	7 Fitzwalter Road, Boreham, Essex. CM3 3DA
Email:	dlagden@dlsolutions.net
Phone Number:	07961048378

1. Restrictions on Sub-Contracting

The GDPR gives Data Controllers a wide degree of control in terms of the ability of the processor to sub-contract. Data Processors require prior written consent. The processor is required to inform the controller of any new sub-processors, giving the controller time to object. If there is an objection, the sub-processing may not continue.
The lead processor in a sub-contracting arrangement is required to reflect the same contractual obligations it has with the controller in a contract with any sub-processors and remains liable to the controller for the actions or inactions of any sub-processor. This letter seeks acknowledgement of and commitment to comply with this requirement:

All staff working for DL Solutions whether employed or self employed will abide by DLSolutions contractual agreements with the Schools. Although we have access to all data, we never remove data from the school sites.

2. Controller/ Processor contract

Data Processor activities must be governed by a binding contract. The binding obligations on the Processor must cover the duration, nature and purpose of the processing, the types of data processed and the obligations and rights of the Controller. There are a number of specific requirements including that the personal data is processed only on documented instructions from the controller, and requirements to assist the controller in complying with many of its obligations. The Data Processor has an obligation to tell the Controller if it believes an instruction to hand information to the Data Controller breaches the GDPR or any other law.
This letter seeks acknowledgement of and commitment to comply with this requirement:

DL Solutions is currently updating contracts with the Schools which details Data Protection further. Pro Forma contract attached.

If there is no contract with the Data Controller, please provide an up to date document setting out current standard of service delivery and terms and conditions under which the service is offered.

N/A

Essex County Council

3. Demonstrating compliance

GDPR requires organisations to demonstrate compliance. Processors are under an obligation to maintain a record of all categories of processing activities. These records must be provided to the Information Commissioner's Office on request. This must include details of:

- the Controllers they act for
- any other Processors
- a Data Protection Officer (DPO)
- the categories of processing carried out
- details of any transfers to third countries
- A general description of technical and organisational security measures.

Processors must assess their need to comply by understanding whether they have fewer than 250 employees. If so, and unless the processing does not pose a risk to the rights and freedoms of individuals, is not more than occasional and does not include special categories of data (sensitive personal data), then the requirements are reduced.
This letter seeks acknowledgement that your organisation has reviewed and understood the level of the requirement on your organisation to comply with the General Data Protection Regulations:

DL Solutions does not take any data away from the schools for processing. We do have access to their Servers' data remotely but do not have the facility to transfer data to\from the School. The Remote Access software we use is GDPR Compliant and has end to end encryption.

4. Security

Processors, like controllers, are required to implement 'appropriate' security measures. What is 'appropriate' is assessed in terms of a variety of factors including the sensitivity of the data, the risks to individuals associated with any processing or breaches of security, the state of the currently available technologies, the costs of implementation and the nature of the processing. These measures might include pseudonymisation and encryption. Regular testing of the effectiveness of any security measures is also required where appropriate. This letter seeks acknowledgement of and commitment to comply with this requirement:

DL Solutions does not take any data away from the schools for processing. We do have access to their Servers' data remotely but do not have the facility to transfer data to\from the School. The Remote Access software we use is GDPR Compliant and has end to end encryption.

Where suppliers have access to school data, please confirm staff vetting procedures, confidentiality clauses in employment contracts and any monitoring/ reviewing/ auditing of their activities. This letter seeks acknowledgement of and commitment to comply with this requirement:

DL Solutions carries out an Enhanced DBS check on all staff and Photo ID is always checked along with their eligibility to work in the UK.

Where suppliers' staff work on a school site, please confirm that DBS certificates have been issued for these member of staff and what procedure are in place for a school to have sight of these certificates.

All DL Solutions staff have recent DBS Checks and are signed up to the Update Service

Where services include disposal of IT hardware – what standard of secure destruction is employed?

If DL Solutions arrange for a company to dispose of Hardware for any schools, we will always ensure that the company can supply the School with a Certificate of destruction.

Data Controllers have a requirement to receive certification of the completed work. This letter seeks acknowledgement of and commitment to comply with this requirement:

The Invoice for work carried out is the confirmation that the work has been completed.

Where devices are removed from site by a Data Processor, how secure are the premises in which they work and what requirements are in place to safeguard any data on the device to which an operative may have access?

The premises where any devices might be taken by DL Solutions will either be occupied or alarmed

5. Breach notification

There are enhanced breach notification requirements on both Data Controllers and Data Processors. Processors are required to notify their relevant controller of any breach without undue delay after becoming aware of it. Controllers have 72 hours to notify the Information Commissioner's Office from the point the breach is detected, therefore reporting from the Processor to the Controller is required well within this time period. Your organisation will to evidence effective process to identify and report breaches of your security measures to the Data Controller promptly, allowing the Controller time to deliberate and comply with the 72 hour rule. This letter seeks acknowledgement of and commitment to comply with this requirement:

DL Solutions does not take any data away from the schools for processing. We do have access to their Servers' data remotely but do not have the facility to transfer data to\from the School. The Remote Access software we use is GDPR Compliant and has end to end encryption.

6. Data Protection Officers

Both controllers and processors are required to appoint DPOs in certain situations, including where they are a public authority or body, where the data processing activities require regular monitoring of data subjects on a large scale, or where the core activities of the processing involve large amounts of special (sensitive) data or data relating to criminal convictions and offences. The primary role of the DPO is to assist the processor with, and advise on, compliance with the GDPR. Processors may also choose to appoint a DPO even if they do not fall into one of the specified categories. Please state above if you have appointed a DPO, or state that you have reviewed the requirement and determined that it is not applicable to your organisation.

7. Transfers to third countries

The processor has to exercise a degree of independence from the controller when deciding whether or not it can transfer personal data to a third country. While processors are required to follow the relevant Data Controller's instructions with regard to the data processing, no matter what those instructions are, they may only transfer personal data to a third country (in the absence of an adequacy decision) if the controller or processor has provided appropriate safeguards and on condition that data subjects have enforceable rights in that country with respect to the data. This letter seeks acknowledgement of and commitment to comply with this requirement:

DL Solutions never transfers any data to a third Country

Signed by	
Print Name	Daniel Lagden
Role within the Organisation	Company Director
Date	10th May 2018

To be completed by Essex County Council

Reviewed by	
Recommendations/notes	
Date	
Date of next review	