

Data Processing Agreement

User Guide

Data Processing Agreement User Guide

Document Purpose

This document provides guidance on using the 'School's Data Processing Agreement' produced by Kent County Council in response to concerns raised by schools about the transfer of personal data to firms providing online services. The Agreement only relates to data processing carried out on behalf of a school. This guide should be read alongside the Agreement, which can be found at the end¹ of this document.

Typically, firms extract data from your school MIS system and transfer this electronically, either directly through your broadband connection, by spreadsheet or by using removable storage media such as CD or memory stick.

Use of this Agreement ensures that both the school ('Data Controller') and Service Provider ('Data Processor') understand their statutory obligations under the Data Protection Act 1998 and follow best practice guidance for information management. It sets out terms and conditions with which the school and its Service Providers should comply and is drafted to take legal precedence over its Service Provider's own terms and conditions, offering valuable additional protection.

Why is a Data Processing Agreement needed?

In order to offer a personalised user experience, Service Providers need details about the user. Simple approaches require little more than knowing which school the user is from, others require Personal Data about the user such as; name, year group, classes. Where Personal Data is requested, it is important to understand that your school remains responsible. A loss of Personal Data by your Service Provider is the responsibility of your school. For this reason, it is important that schools understand where their data is being held, who can access it, and how secure it is.

This Agreement is designed to be used whenever a school buys a service that involves the transfer of Personal Data to a Service Provider for whatever purpose. Service Providers typically expect Headteachers to sign their Data Processing Agreement as a condition of service. However, these vary considerably in quality and typically do not offer a school appropriate protection.

Reputable Service Providers should have a few concerns in signing the document. Typical services that extract data include Learning Platforms, such as RM Living Library and Encyclopaedia Britannica, Virtual Learning Environments (VLE's) such as Moodle and online content providers such as Online Homework Help.

Using this Data Processing Agreement

The Data Processing Agreement sits alongside a commercial contract with a Service Provider, and doesn't replace it. Avoid accepting a Service Provider's standard Data Processing Agreement as this often transfers liability and risk back to the school, and may not meet your expectations for the security and treatment of the data you control. Remember, you are the Data Controller, and the responsibility is yours.

The Data Protection Act 1998 sets out a number of principles for data collection and processing. It is important to ensure your school's privacy notice states the purpose of any data processing carried out on behalf of your school. (A revised Privacy Notice that covers third party processing is available on Kent Trust Web).

Service Providers often seek to collect more data than is needed for the specified purpose. This may be to simplify extraction by taking a whole dataset rather than trying to filter data before extraction. This does not comply with Data Protection Principles that state: 'Personal Data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed'. For this reason the Data Processing Agreement includes a schedule of individual data items being processed. There should be a legitimate reason for each item. SIMS reports can be customised to achieve this.

The school's Data Processing Agreement is not appropriate for use where web-hosting is the only service. In these cases data is controlled directly by the purchaser. Care needs to be taken though to check that data does not leave the country and that appropriate security is in place to protect users. This is particularly relevant where schools use hosting to provide their own services, e.g. Moodle (VLE).

Online services are frequently hosted abroad and legal protections only relate to data held and processed within the European Economic Area (EEA). Whilst a number of countries are classed as 'Safe Harbor's', Personal Data should not be transferred to a country or territory outside the EEA.

The Agreement sets out the right for a school to audit a Service Provider's facilities, procedures and documentation. Where problems are identified they must be rectified before further data is processed. Do not be afraid to ask questions, such as where your data is physically stored, who has access and why, and how is it backed-up. It is also vitally important to ask what would happen in the event the Service Provider ceases trading.

The use of CD's or USB memory sticks to transfer personal data must follow best-practice guidelines, and be treated as a last resort. Email security cannot be guaranteed so personal data should not be sent in the text of an email. A separate attachment may be used provided it is password protected or encrypted (with the password sent in a separate email).

The agreement does not terminate when the associated commercial contract ends. There is an obligation on the Service Provider to comply with your schools data retention policy. This ensures that important data, such as assessment records and pupil's work are handed back to the school in a usable format.

In the event of a Service Provider is in breach of the Agreement and fails to rectify within a reasonable time or ceases trading, the school is entitled to end the Agreement and by doing so would have good grounds to end the commercial contract.

Schedules to this Data Processing Agreement

Schedule 1 should include a copy of the commercial contract and its terms and conditions. Where a contract contradicts terms set out in Data Processing Agreement, the Data Processing Agreement takes priority.

Schedule 2 lists the Data Items being extracted from the School Management Information System. This ensures all parties are aware of what data is being processed. If data items are added or removed during the life of the agreement, Schedule 2 should be agreed and amended.

Use of Appendix A is optional, and provides additional clarity over data-flows between organisations.

Glossary

What is Data Processing?

Data Processing is the obtaining, recording or holding of information including any operations carried out using the data. In relation to this Data Processing Agreement it is the transferring of Personal or Sensitive Personal Data processed from the school to the external Service Provider.

Data Controller

A person who determines the purpose and the manner in which any Personal data is processed.

Data Processor

In relation to Personal Data means any person who processes or transfers the data on behalf of the Data Controller.

Data Subject

This is the individual who owns the Personal Data being processed, it is data about them.

ICO

The Information Commissioner's Office is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals

Personal Data

This refers to Data which relates to a living individual who can be identified from the information held by the Data Controller. For example name, address and date of birth.

Sensitive Personal Data

This is Personal Data which consists of information such as; race, religious and political beliefs, physical or mental health conditions, sexual life and any offences committed or allegedly committed.

Purpose

This is the reason you have for processing and storing the data.

Service Provider

Is a company which provides a usable service to other organisations.

Relevant Information

Principles of the Data Protection Act 1998

1. Personal Data shall be processed fairly and lawfully and shall not be processed unless at least one of the conditions in Schedule 2 of the Data Protection Act is met or in the case of Sensitive Personal Data, one of the conditions in Schedule 3 of the Data Protection Act is 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. Personal Data shall be processed in accordance with the rights of Data Subjects under this Act.
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 unless that country or territory ensures an adequate level of protection for the rights and freedoms of the Data Subjects in relation to the processing of Personal Data.

ICO conditions for fair processing

At least one of the following conditions must be met before processing Personal Data:

- An individual Data Subject, e.g. learner or staff member, has either given consent for their personal data to be processed or there is a statutory obligation (e.g. school census).
- Processing is necessary because the Data Subject has entered into a contract or requested something to be done so they can enter into a contract.
- Processing is necessary in order to meet a legal obligation.
- Processing is needed in order to protect the Data Subject. (*Note: This condition only applies in matters of life and death, for example, access needed by an A&E department to an individual's medical history in a life threatening situation*).
- Processing is necessary for administering justice or for exercising statutory, governmental or other public functions
- Or if the processing is in compliance with the 'legitimate interests' condition (see ICO website for conditions).

Frequently Asked Questions

What if a Service Provider refuses to sign?

If a Service Provider refuses to sign the Agreement then it would be appropriate to ask them to give their reasons since most of the agreement conditions restate statutory requirements. Issues such as Indemnity (10.1) can be negotiated however, and the agreement amended if required.

Is this document a legal requirement?

No, but the agreement helps schools to understand their obligations under the Data Protection Act 1998 and makes it clear how these will be met by any Data Processor acting on their behalf.

Are service providers aware of the Agreement?

Several major firms were consulted, and the only objections were in regard to the indemnity clause (10.1). Our advice to schools is to negotiate this point if your service provider objects.

Where can I download the School's Data Processing Agreement

The Schools Data Processing Agreement can be found at the following web address:

Author: Danielle Jones – Digital Curriculum Officer © Kent County Council

http://www.kenttrustweb.org.uk/UserFiles/CW/File/Advisory_Service_ICT/Digital_Curriculum/SchoolsDataProcessingAgreement_300910.doc