Class Systems
Language School Software

+44(0)1202 734363
sales@infospeed.co.uk
www.class-systems.com

Infospeed Ltd.

Data Retention Policy

March 2018

In partnership with

ENGLISHUK

feltom
FEDERATION OF ENGLISH LANGUAGE TEACHING ORGANISATIONS MALTA

flywire

guided e-learning

+44(0)1202 734363
sales@infospeed.co.uk
www.class-systems.com

1. Introduction

This policy is designed to give clear guidance on how customer and staff data should be stored and backed up and when such data should be deleted.

2. What Data Categories are covered by this agreement?

This policy covers the following data categories as outlined in our Customer Data and Employee Data Protection Policies

Data Ref.	Type of Data	Purpose of Data
Data-001	Customer Data - Multi-Tenancy Cloud - for the purposes of Data Patching - Customer Class Database	Data Required for development work e.g. Data Patching
Data-002	Customer Data - Self Hosted - for the purposes of Data PatchingCustomer Class Database	Data Required for development work e.g. Data Patching
Data-003	Employee Data	Staff Employment

3. Why is data requested and stored on our systems?

As a last resort it may be necessary for the Development team to request a copy of the customer's database which is downloaded from the source and placed upon Infospeed servers. This allows Development to replicate errors without impacting a customer's live environment. It also allows the use of additional debugging tools and comparing actions against the Class.net source code. The latter cannot be replicated on a customer site – even if they have a test environment available.

4. When is data downloaded from customer systems?

Downloading the data from a customer should be considered a last resort where the fault cannot be found or replicated within the customers testing system (where applicable)

+44(0)1202 734363
sales@infospeed.co.uk
www.class-systems.com

5. How is the data requested?

Data can only be requested from the Engineering department once a ticket has been raised on the incident management system that shows that all other options for resolution have been attempted.

The Engineering department then contacts the customer to seek approval for database retrieval

6. Will a Data Protection Risk Assessment be required?

In most cases it will not be necessary to carry out a Risk Assessment for standard requests. Each data request will be logged onto our Data Compliance Form and where a Risk Assessment is deemed necessary this will be carried out.

7. How long is the data stored on our systems?

Data Ref.	Review Period	Retention Period
Data-001	2 weeks	No longer than 48 hours after the closing of the case.
Data-002	2 weeks	No longer than 48 hours after the closing of the case.
Data-003 (Staff data)	Annually	7 Years

If the case takes in excess of 2 weeks to be resolved the Engineering team liaise with the developer that has requested the database to see if an extension of data retention is required. We will typically also request an expected completion date for the database retention so that we can field this back to the customer if they request it.

8. Backing up customer data.

We purposefully DO NOT take snapshots or system state backups of customer data on our SQL Servers during the retention period.

+44(0)1202 734363
sales@infospeed.co.uk
www.class-systems.com

9. Data Deletion

Once data has been identified for deletion it will be deleted in a manner that is unrecoverable.

As follows:

Data Ref.	Deletion Type	Security Measures taken
Data-001	Full Permanent Delete	Files are deleted and then permanently erased by utilising a 2-pass HMG Infosec Standard 5 (IS5) data wipe.
Data-002	Full Permanent Delete	Files are deleted and then permanently erased by utilising a 2-pass HMG Infosec Standard 5 (IS5) data wipe.
Data-003 (Staff data)	Full Permanent Delete	Files will be deleted from Current HR Database and Filing systems