Vizi Education - IT Security policy

Amendment history

1) Created - 25/07/2017 - Michael Williams
2)

Introduction (Ext)

Purpose

The purpose of the IT Security Policy is to outline the IT security protocols for Vizi Education Ltd (The Company). The Policy gives details on the guidelines, procedures and specification of the IT Security implemented at The Company.

Distribution

This document is intended for distribution to all employees of The Company. Elements of The Policy that are marked 'External' are intended for distribution to all users of the software.

Roles and Permissions (Ext)

Vizi Roles

The software has four standard roles that a user can be allocated - Admin, Teacher, Student and Parent. Upon allocation of a role, the specific permissions of the role can be manipulated to suit the exact requirements of the user, but will remain in the boundaries of that role. For example one teacher may be able to access all forms for their school and another may be limited to only the forms they teach. However a teacher will never be able to create users - permissions limited to the administrator role.

Teacher

A teacher can access data associated with multiple students, create assignments, enter marks and share information via the timeline. See the table of

Student

A student has access only to details relating to themselves and information directed to them by teachers. Students will not be able to access other student data in any scenario.

Parent

A parent has access only to details relating to an allocated or allocated students and information directed to them by teachers. Parents will not be able to access any other student data other than the for the students they are allocated too.

Vizi Permissions

Student/Parent

Student and parent permissions are limited to the role definitions above.

Teacher

Teacher permissions are dictated by the groups and collections that they are a teacher for. If a teacher is attached to a group they will have read/write permissions for that group's performance data.

If a teacher has been attached to a collection, they will get read permissions for the performance data of the groups and users within that collection.

All teachers will have read permissions for general information on collections, groups and users, however, this does not include performance data.

Administrator

Teachers can have the administration permission attached to their user profile. This will give that teacher access to the admin tools menu which is used to setup Vizi parameters (see the Vizi guide - Setup) and

edit non-performance related information (student details and group allocations for example). It is suggested this is limited to IT personnel to control data integrity.

Data Security

Data Storage

Location

All data collected by Vizi is stored on Amazon Web Server (AWS) UK. The UK facility is located in .

Data protection act 1998

The Company complies fully with the Data Protection Act 1998 (DPA) and is a member of the ICO. All personal data is stored under full compliance with the DPA.

Please refer to following link for details of the

https://ico.org.uk/for-organisations/guide-to-data-protection/

Amazon Web Server (AWS) detail

In this case, AWS is responsible for securing the underlying infrastructure that supports the cloud, and Vizi are responsible for anything you put on the cloud or connect to the cloud.

Please refer to the following document for details on AWS's IT security policy:

https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

Please note the following key points:

- Physical security
    - There is three phase entry to AWS locations
- Local Security

Please refer to the following page for details on AWS's compliance with global data security certificates:

https://aws.amazon.com/compliance/

Data centre location

Vizi has chosen to host client data in the newly established UK AWS data centres.

Data retention and deletion

Data retention

Data will be retained for

Data deletion

Data backups

Vizi has a constant mirrored database on a separate AWS server that acts as an immediate and complete backup should the primary server go down.

There is a supplementary weekly backup of the complete Vizi database to a separate provider to the primary AWS storage.

Web Security

Encryption

Vizi is encrypted with HTTPS ensuring communication between users and vizi is kept secure and data can not be tampered with or intercepted.

Automated logout

A user is logged out after 10 minutes of inactivity. The user must then re-enter their password to access their account.

Change Control

Code maintenance

Audit trial

Test environment

Change Types

Testing

User Access testing

All changes are subject to

Password policy

Teacher Password Policy

A teacher's passwords will adhere to the following criteria:

- 10 or more characters in length
- Password changed every three months
- The previous five passwords used by the user cannot be reused

Administrator Password Policy

Administrator accounts will use a two factor authentication to login. An administrator will login normally, following the same password parameters as teachers. To access the admin tools area of Vizi the user will be asked to enter a four digit pin. This will adhere to the following criteria:

- xx
- xx
- xx

Student and Parent Password Policy

Student and Parents will adhere to the following criteria:

- 7 or more characters in length
- Include a special character
- Include upper and lower case letters
- Password changed every six months
- The previous three password used by the user cannot be reused

Disaster recovery

AWS disaster recovery reference

Business Continuity

AWS business continuity reference