



Data Protection Impact Assessment

Name Of School: The Willows Primary School

Assessment Carried Out By: Kirsten Warren

Name Of Project/Technology/System

Seesaw Learning

Aims Of The Project/Technology/System

To increase student and parent engagement with school work, it allows students to use tools to take pictures, draw and record videos whilst also providing class activities for teachers to utilise or to create their own. Families can view the students work and leave comments.

Use Of Personal Data

Seesaw collects personal data from teacher/ parent/ family member/ school administrators.

Information that Seesaw collect are:

- **Account Information:** this may include, name, email address, password, telephone number and profile picture.
- **Journal content:** this may include, photos, drawings, files, notes, hyperlinks and other ways of documenting student learning, comments on posts in your class journal which may be text, or if the school allow Seesaw to access the microphone on your device, voice recordings.
- **Messages:** collects messages that are sent and received in Seesaw by teachers, family members and students.
- **Activities:** teachers may use Seesaw to create activities for the students to use. This may include text or voice instructions for how to complete the activity.

- **Activity author profiles:** schools who choose to publish activities to the Community Activity Library or the Activity Library managed by their school. This may include name and profile picture, as well as school name and location.
- **Communications:** which is any information the school send directly to Seesaw, such as emails.
- **Log Data:** when the school use Seesaw, they receive log data such as IP address (used to provide tailored marketing and information), browser type, operating system, device information, and mobile

Reasons For Processing

By using Seesaw, students will be able to engage more with their learning leading to better quality education which the school has a duty to provide. It also allows teachers to get a better idea of how a student is performing and lets families see how their children are learning which will also improve student education.

To keep parents up to date with their child's progress and to open the lines of communication.

- Allow the school to access and use the service by verifying identity and storing Journal content, activities and messages
- Provide teachers, schools and family members with customer support
- Notify you about activity on and updates to your account or your child's account (if the school have indicated on their privacy settings that they would like notifications)
- Research, understand and analyse trends of users to improve and develop new features.
- The school will obtain consent from parents/students before personal data is shared with Seesaw.

The lawful reason for processing the data will be by consent.

SeeSaw require that teachers or schools get parental consent before using Seesaw with children who are under the age when they can grant consent on their own. This age in the UK is 12 years old. If the school are aware Seesaw is collecting information from a student without parental consent, they would like them to be contacted immediately at help@seesaw.me and they will delete the data.

Impact And Risks To Personal Data

None of the data collected by Seesaw is particularly sensitive in nature however as users can upload content themselves the overall risk would have to be high as there is no restriction on what can be uploaded although it is possible to be in violation of the terms of service.

Data will be collected on an ad-hoc basic due to the nature of the platform with Seesaw keeping data for as long as the accounts are in use. Seesaws terms of service state that if accounts have not been used for one-year Seesaw reserves the right to delete said accounts and all associated data although they do reserve the right to delete the account with no notification if in breach of the terms. Otherwise a notification will be sent to a teacher or school associated with the accounts so that an archive copy of the data can be downloaded prior to deletion.

Users whose personal data will be affected are students, teachers, parents and family members. Parents will usually only see their own child's information/pictures. However, group photographs will contain other children.

There is a low risk to student/ staff/ parent/ family member privacy if an unauthorized user depending on what they have chosen to include in their profile, say for example; a photo of their face used for a profile picture was accessed or if a document or video was uploaded containing personal information.

The school's reputation could be damaged should any data be lost or stolen, as it is the School's responsibility to safeguard personal data. There is an inherent overall risk to the storing of data in data centres and its transmission over the internet along with its default storage in the US unless changed. However, their privacy policy states that accounts that have not been used in seven years will go through the deletion process. Once an account has been deleted Seesaw may still hold on to data for up to 60 days to provide customer support and prevent accidental deletion.

User accounts on Seesaw can be deleted sooner than stated above after a web form has been filled in requesting that an account be deleted.

Seesaw contracts with the Amazon Web Service (AWS) to provide data centre and server hosting services for Seesaw. This means things like making sure the Seesaw servers are always fast regardless where in the world you are accessing Seesaw.

The risk is considered to be low because of the security measures Seesaw have in place to protect personal data.

Minimal data will be shared and no special category data will be shared with Seesaw.

Will This Information Be Shared With Third Parties?

Seesaw states that although they use third-party analytics to see what buttons are clicked and which pages are visited: "In no circumstances are any data you have shared with Seesaw (such as your Account Information or Journal Content) shared with these services. In addition, these services are contractually obligated only to use data about your usage of Seesaw to provide analytics services to us and are prohibited from sharing it or using it for other purposes."

SeeSaw will not share the school's information with third parties.

Seesaw protects personal data by using TLS 1.2 at the network level for the transmission of account information and journal content. That data is also encrypted at rest with all password used being salted and hashed. In terms of access to personal data that may have been uploaded by students, its access control is set by teachers with it being set to private by default.

The company conduct 3rd party security audits to ensure the integrity of their systems with internal monitoring for inappropriate access and any security breaches.

The data centres used have 24/7 monitoring with data being stored redundantly with distributed locations enabling high levels of availability and access. Access to personal data is restricted to specific staff who need to have a business need to do so with staff having a background check before starting their job. They also sign a non-disclosure agreement and have access to systems and data removed upon leaving the job. Customer data is also not stored on individual employee computers.

Seesaw use a small number of third-party services in order to operate and improve Seesaw.

To host and deliver Seesaw:

- Amazon Web Services (Data centre management)
- Launch Darkly (Beta testing support)

To communicate with teachers, families and administrators

- Autopilot (Sending emails)
- Boomerang (Sending emails)
- Mailchimp (Sending emails)
- Mailgun (Sending emails)
- Twilio (Sending text messages)
- Versal (Provide online courses)

To run their internal operations

- Zendesk (Software for customer support)
- Ada (Software for customer support)
- Shopify (Operating the Seesaw store)
- Salesforce (Manage customer relationships)
- Outreach (Organise communications with schools)
- Wufoo (Collect interest in Seesaw for schools)
- SaaSOptics (Manage internal finances)
- Quickbooks (Manage internal finances)
- Survey Monkey (Conduct surveys and user research)

Google (Manage emails, calendars and documents)

What Steps Will Be Taken To Protect The Data?

A Data Processing Agreement between the school and Seesaw will be completed. Parental consent forms will also be given to parents/ family members. Students and Staff are told not to share their account details with others.

Parental consent for the app will be required as photographs of their children may be seen by other parents and SeeSaw.

The app will be password protected.

Parents or guardians can withdraw their consent at any time.

Seesaw has put a number of measures in place to protect the integrity of the students information including:

- Data encryption in transit
- Encryption of Journal Content (e.g. the photos, video, audio, and other content the school add to Seesaw) at rest
- Seesaw uses SSL security at the network level to ensure all account information and journal content is transmitted securely
- All passwords are salted and hashed using PBKDF2
- Seesaw routinely conducts third party security audits to verify the security and integrity of their systems and internal controls.
- Account information is stored in access-controlled data centres operated by industry leading partners with years of experience in large-scale data centres.
- All user information is stored redundantly and backed up in geographically distributed data centres. They utilize multiple distributed servers to ensure high levels of uptime and to ensure that they can restore availability and access to personal data in a timely manner.

- They have adopted an internal data access policy that restricts access to personally identifiable information to a limited number of employees with a specific business need (such as for technical support).
- All employees at Seesaw undergo a background check before beginning employment at Seesaw, sign a nondisclosure agreement, and immediately lose access to all internal systems and data when terminated. --
- No customer information is stored on individual employee computers.
- They routinely monitor their systems for security breaches and attempts at inappropriate access.
- They use encrypted QR codes for family and student access to journal content.
- Seesaw has taken the Student Privacy Pledge.
- Seesaw complies with the EU - U.S. Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use and retention of personal information from European Union member countries. Seesaw has certified that it adheres to the Privacy Shield Privacy Principles of notice, choice, and accountability for onward transfer, security, data integrity, access, and enforcement and liability.

Protecting the schools privacy is fundamental to SeeSaw’s mission and business. The following summarize their promises to the school.

- We never sell your data or student data.
- We never advertise in Seesaw.
- We don’t own the content you add to Seesaw.
- Student work is private to the classroom by default.
- We use the latest security industry best practices to protect you.
- We are transparent about our practices and will notify you if things change.
- We are compliant with FERPA, COPPA, GDPR, and the Australian Privacy Act.

Seesaw will delete an account and all content associated with the account if the account has not been accessed for more than 7 years. Prior to deleting the abandoned account, Seesaw will notify the teacher

Any Other Factors To Consider

Compliance Statement

I can confirm that this data protection impact assessment has been completed to the best of my knowledge and that Seesaw Learning complies with the data protection principles under the GDPR.

Signed:

Date: