Data Protection Impact Assessment (Seesaw)

Caslon Primary Community School operates a cloud based system or 'hosted solution', called Seesaw. Access to Seesaw is through the internet. Information is retrieved from Seesaw via the Internet, through a web-based application, as opposed to a direct connection to a server at the school. Access to Seesaw is through a web browser. As such Caslon Primary Community School must consider the privacy implications of such a system. The Data Protection Impact Assessment is a systematic process for identifying and addressing privacy issues and considers the future consequences for privacy of a current or proposed action.

Caslon Primary Community School recognises that using a 'hosted solution' has a number of implications. Caslon Primary Community School recognises the need to have a good overview of its data information flow.

The Data Protection Impact Assessment looks at the wider context of privacy taking into account Data Protection Law and the Human Rights Act. It considers the need for a cloud based system and the impact it may have on individual privacy.

The school needs to know where the data is stored, how it can be transferred and what access possibilities the school has to its data. The location of the server is important to determine applicable law. The school will need to satisfy its responsibilities in determining whether the security measures the cloud provider has taken are sufficient, and that the rights of the data subject under the UK GDPR is satisfied by the school.

Caslon Primary Community School aims to undertake a review of this Data Protection Impact Assessment on an annual basis. A Data Protection Impact Assessment will typically consist of the following key steps:

1. Identify the need for a DPIA.
2. Describe the information flow.
3. Identify data protection and related risks.
4. Identify data protection solutions to reduce or eliminate the risks.
5. Sign off the outcomes of the DPIA.

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

What is the aim of the project? – Caslon Primary Community School

A specific number of teaching staff have been identified as requiring access to the system. Access is dependent on job role and need. Seesaw provides a level of access to facilitate this requirement.

Seesaw is a hosted system which means that all updates, maintenance and management can be performed in a central location by Seesaw.

Seesaw is a hosted platform that provides a number of learning tools to facilitate remote learning by students. Students can create a journal by adding media-rich content such as photos, drawings, videos, files, notes or web links. Teachers can create completely new class activities or utilise from the existing activities and resources, provided for teachers to adapt for their own use. Teachers approve student content before it is made available to the class activity.

Caslon Primary Community School hopes to provide the flexibility of remote learning by adopting the platform.

By employing Seesaw, the school aims to realise benefits by adopting a common platform to improve processes, secure remote access and identifying issues which can then be shared across all those staff that have access through centrally-managed training.

Caslon Primary Community School will undertake the following processes:

1. Collecting personal data
2. Recording and organizing personal data
3. Storing personal data
4. Copying personal data
5. Retrieving personal data
6. Deleting personal data

By opting for Seesaw the school aims to achieve the following:

1. Management of sensitive pupil information in one place
2. Security and integrity of sensitive data through a secure document vault
3. Storage of information electronically rather than manually
4. Recording information and building a chronology around the pupil
5. Providing bespoke reports for different audiences, e.g. Parents or agencies
6. Identifying trends and patterns
7. Ability to add information from staff across the school
8. Secure access across all devices wherever the setting

Cloud based systems enable the school to upload documents and other files to a hosted site to share with others within school. These files can then be accessed securely from a PC in the school.

Seesaw cannot do anything with the school's data unless they have been instructed by the school. The schools Privacy Notice will be updated accordingly. The school is the data controller and Seesaw is the data processor.

Caslon Primary Community School has included Seesaw within its Information Asset Register.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

The Privacy Notices (pupil) for the school provides the legitimate basis of why the school collects pupil data. Specifically, this relates to health and safety and safeguarding of vulnerable groups. Seesaw is referenced in the respective Privacy Notices.

How will you collect, use, store and delete data? – Seesaw collects information from pupil records, Special Educational Needs (SEN) records and behavior records. Student details are added individually through the secure portal, or bulk records can be uploaded via a CSV file. Staff records are added individually through the secure portal. The information will be stored in Seesaw. The information is retained according to the school's Data Retention Policy. A facility is also available to create classes through Clever Sync or ClassLink.

What is the source of the data? – Pupil information is collected via registration forms when pupils join the school, pupil update forms the school issue at the start of the year, Common Transfer File (CTF) or secure file transfer from previous schools. Pupil information also includes classroom work, assessments and reports. SENCO records, Education Health and Care Plans, Pupil Records, and Common Assessment Framework.

Will you be sharing data with anyone? – Caslon Primary Community School may share information with education professionals including the SENCO, Headteacher, Senior Leadership Team (SLT), Governors, Ofsted, the local authority. However, this does not mean that Caslon Primary Community School shares Seesaw access to the third parties.

What types of processing identified as likely high risk are involved? – Transferring 'special category' data from the school to the cloud. Storage of personal and 'special category data in the Cloud.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

What is the nature of the data? – Pupil data relates to personal identifiers and contacts (such as name, tutor, teaching group membership). Information that is processed (but not limited to): pupils' names, pupils' data (class name, grade level, sign in mode, a unique student ID). Email address is only required if email is used as the sign in method.

Workforce data relates to personal information (such as name, email address, class groups that have been assigned to the teacher). Only enough information is collected for the school to create a login account for the member of staff and assign the student groups they are assigned to.

Special Category data? – Data revealing racial or ethnic origin, medical details are collected by the school and contained in Seesaw. The lawful basis for collecting this information relates to Article 9 2 (g) *processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject*.

How much data is collected and used and how often? – Personal details relating to pupils are obtained from parent/pupil information systems. Additional content is obtained from classroom/teacher observation/agency partners. This also includes recorded information and reports.

How long will you keep the data for? – The school follows the good practice in terms of data retention as set out in the IRMS Information Management Toolkit for Schools and the schools data retention policy.

SEND information is transferred to the receiving school as part of the pupil record. This is signed for by the receiving school. This is then kept by the receiving school from DOB of the child + 31 years then reviewed.

Scope of data obtained? – How many individuals are affected? The number of students that will take part in the Seesaw programme with be (210 pupils). The geographical area covered is from pupils aged 4 (Reception) to age 11 (Year 6).

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

What is the nature of your relationship with the individuals? – Caslon Primary Community School
collects and processes personal data relating to its pupils to ensure the school provides education to its students with teaching staff delivering the National Curriculum.
It also collects and processes personal data relating to its pupils to manage the parent/pupil relationship. Personal data is collected for the workforce to assist with the creation of login accounts dependent on job role.

Through the Privacy Notice (Pupil) and (Workforce) Caslon Primary Community School is committed to being transparent about how it collects and uses data and to meeting its data protection obligation.

How much control will they have? – Not all staff will have access to Seesaw. The school can restrict access to Seesaw so that only designated staff only see information that is relevant to them. Access to the data held on Seesaw will be controlled by username and password.

Additionally, whilst Seesaw works on any device with access to the internet, staff that are granted access to the system will have to utilise an additional password of their own, which is only shared between authorized members of staff at the school. School administrators have full access to the system, which are defined by permissions. Mobile apps are also provided for a number of different platforms so that students can access the Seesaw system from a mobile device.

Do they include children or other vulnerable groups? – All of the data will relate to children. The information will relate to learning assessment, etc.

Are there prior concerns over this type of processing or security flaws? – All data is secured in transit using modern SSL standards used throughout the industry.

Caslon Primary Community School recognises that moving from an existing electronic system to an alternative electronic system which holds sensitive personal data in the cloud raises a number of UK General Data Protection Regulations issues as follows:

- **ISSUE:** Seesaw will be storing personal data
  RISK: There is a risk of unauthorized access to information by third parties
  MITIGATING ACTION: Seesaw school data is stored on approved and compliant cloud infrastructure. Access to all parts of the infrastructure is available to Seesaw staff on a need to know basis and access is always revoked as soon as a member of staff no longer needs access or leaves the company. User access is based on individual usernames and passwords

- **ISSUE**: Transfer of data between the school and the cloud
  RISK: Risk of compromise and unlawful access when personal data is transferred.
  MITIGATING ACTION: All connections to a Seesaw installation are encrypted over SSL. The https:// (instead of the normal http://) in the school's browser's address bar denotes a SSL connection, which means any data transferred is encrypted before being sent. The SSL certificate also allows the school's computer to verify that the Seesaw server is the server it says it is. Connections are encrypted with 256-bit AES encryption / TLS 1.3. AES encryption is a US government standard for encryption, and 256-bit is the highest level available

  In addition, journal content (created by the school) is encrypted at rest on the Seesaw servers along with any communication between Seesaw and the other third-party cloud service providers

  All staff employed by Seesaw who work on Seesaw (including agents and subcontractors) shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty or otherwise), and shall not permit any person to Process the Data who is not under such a duty of confidentiality. Authorised persons shall only access the data only as necessary for the permitted purpose

- **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: Seesaw utilises geographically distributed data centres. In addition, it uses multiple servers to ensure high levels of uptime and performance

  Seesaw employs a third-party to conduct regular third-party security audits who complies with best industry standards. Seesaw has audit trails in place that enable the internal teams to monitor who is accessing user data

- **ISSUE:** Cloud solution and the geographical location of where the data is stored
  RISK: Within the EU, the physical location of the cloud is a decisive factor to determine which privacy rules apply. However, in other areas other regulations may apply which may not be Data Protection Law compliant
  MITIGATING ACTION: Seesaw servers are hosted in the United States. Seesaw uses the EU-US Privacy Shield for the basis of its data protection standards compliance. Due to the recent decision making the EU-US Privacy Shield invalid, Seesaw provides a Data Processor Agreement which forms the basis of a Standard Contractual Clause (SCCs) which provides Seesaw and its customers the lawful basis to transfer and process data

  As part of the EU-US Privacy Shield ruling the European Court of Justice (ECJ) decided that Standard Contractual Clauses, remain valid

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Where it is necessary to access school data only approved Seesaw staff can access it. All staff have background checks and sign non-disclosure agreements; access to systems is immediately revoked when their contract of employment is terminated

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Seesaw follows the school's data retention policy; data is managed and updated by the school. If required, Seesaw will comply with a school request to delete its data; Seesaw will ensure that this is complied with, within 60 days

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Seesaw has policies and procedures in place to ensure schools are notified in the event of data breaches as required by UK GDPR

  If the school becomes aware of a breach it will contact the named Seesaw contact concerning security issues, serious or minor. In the event of a serious incident, the school will have the full support of the company's technical team as a matter of priority until the issue is resolved

- **ISSUE:** Data is not backed up
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Seesaw has a disaster recovery plan; data is distributed across geographically different locations to minimize the risk of loss of data. It utilises multiple distributed servers to ensure high levels of uptime and to ensure that Seesaw can restore availability and access to personal data in a timely manner

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Seesaw servers are hosted in the United States. Post Brexit, Seesaw and its customers will continue to rely on Standard Contractual Clauses for the transfer and processing of personal data

- **ISSUE:** Subject Access Requests
  RISK: The school must be able to retrieve the data in a structured format to provide the information to the data subject
  MITIGATING ACTION: Seesaw has the capability to provide the schools with access to the data stored within. Where Subject Access Requests are made for specific areas of school data Seesaw can either provide, or will provide, means for authorised client users to carry out activities directly

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: As Data Controller the school maintains ownership of the data. Seesaw is the data processor

- **ISSUE:** Cloud Architecture
  RISK: The school needs to familiarise itself with the underlying technologies the cloud provider uses and the implications these technologies have on security safeguards and protection of the personal data stored in the cloud
  MITIGATING ACTION: Account information is stored in highly secure access-controlled data centres, with around-the-clock monitoring, operated by Amazon Web Services (AWS) who have a substantial background and certifications in operating data centres. All user information is stored redundantly and backed up in geographically distributed large-scale data centres

  The school should maintain ownership of the Cloud technologies used ensuring the current and future technologies enable UK GDPR compliance

  Seesaw can also scale to meet increased platform demand, by scaling capacity as required

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Amazon Web Services hold compliance with ISO/IEC 271001:2013, 27017:2015 and 27018:2019. Seesaw are registered with the ICO, registration number ZA525965

  Seesaw Learning Inc has an ICO Self Certification Statement

  ISO 27001: is one of the most widely recognized, internationally accepted independent security standards

  ISO 27017: is an international standard of practice for information security controls based on ISO/IEC 27002, specifically for Cloud Services

  ISO 27018: is an international standard of practice for protection of personally identifiable information (PII) in Public Cloud Services

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

The school moving to a cloud based solution will realise the following benefits:

1. Management of sensitive pupil information in one place
2. Security and integrity of sensitive data through a secure document vault
3. Storage of information electronically rather than manually
4. Recording information and building a chronology around the pupil
5. Providing bespoke reports for difference audiences, e.g. Parents or agencies
6. Identifying trends and patterns
7. Ability to add information from staff across the school
8. Secure access across all devices wherever the setting

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

The views of senior leadership team will be obtained. Once reviewed the views of stakeholders will be taken into account

The view of YourIG has also been engaged to ensure Data Protection Law compliance

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

The lawful basis for processing personal data is contained in the school's Privacy Notice (Pupil). The lawful basis includes the following:

- Health and Safety at Work Act
- Keeping Children Safe in Education
- Safeguarding Vulnerable Groups Act
- Working together to Safeguard Children Guidelines (DfE)

The school has a Subject Access Request procedure in place to ensure compliance with Data Protection Law

Seesaw will enable the school to uphold the rights of the data subject; the right to be informed; the right of access; the right of rectification; the right to erasure; the right to restrict processing; the right to data portability; the right to object; and the right not to be subject to automated decision-making; these rights will be exercised according to safeguarding considerations.

The school will continue to be compliant with its Data Protection Policy.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
Data transfer; data could be compromised	Possible	Severe	Medium
Asset protection and resilience	Possible	Significant	Medium
Data Breaches	Possible	Significant	Medium
Post Brexit (GDPR noncompliance)	Possible	Significant	Medium
Subject Access Request	Probable	Significant	Medium
Upholding rights of data subject	Probable	Significant	Medium
Data Retention	Probable	Significant	Medium

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no
Data Transfer	Secure network, end to end encryption	Reduced	Medium	Yes
Asset protection & resilience	Data Centre in EU, Certified, Penetration Testing and Audit	Reduced	Medium	Yes
Data Breaches	Documented in contract and owned by school	Reduced	Low	Yes
Post Brexit	Standard Contractual Clause in place	Reduced	Low	Yes
Subject Access Request	Technical capability to satisfy data subject access request	Reduced	Low	Yes
Upholding rights of data subject	Technical capability to satisfy rights of data subject	Reduced	Low	Yes
Data Retention	Implementing school data retention periods as outlined in the IRMS Information Management Toolkit for Schools and data retention policy	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	**Headteacher/Governing Board**	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	**Headteacher/Governing Board**	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Yes	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Technical recommendations to be clarified with third party as follows: *(1)* Does Seesaw provide the technical capability to ensure the school can comply with rights of access and subject access requests *(i.e. rights to request access, rectification, erasure or to object to processing?)* What is the cloud based solution chosen where data processing/storage premises are shared? *(Data is stored within an environment which utilizes state of the art network security, electronic surveillance, physical security and multi factor access control systems along to protect client data?)* *(2)* Does the functionality exist to enable the school to apply appropriate data retention periods? *(i.e. the period for which personal data will be stored)* (3) What certification does Seesaw provide? *(e.g. ISO 27001 certified, ICO registration)*		
DPO advice accepted or overruled by:	No	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	**Headteacher/Governing Board**	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	**Headteacher/Governing Board**	The DPO should also review ongoing compliance with DPIA