# Data Protection Impact Assessment (SISRA Analytics)

Summerhill School operates a cloud based system, called SISRA Analytics (SISRA Limited). Access to SISRA Analytics via the Internet, through a web-based application, as opposed to a direct connection to a server at the school. Access to SISRA Analytics can be through a PC, smartphone, iPad and tablet. As such Summerhill 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. Summerhill School recognises that using a cloud based system has a number of implications Summerhill 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.

Summerhill 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.

# Contents

Step 1: Identify the need for a DPIA ..... 3
Step 2: Describe the processing ..... 5
Step 3: Consultation process ..... 12
Step 4: Assess necessity and proportionality ..... 13
Step 5: Identify and assess risks ..... 14
Step 6: Identify measures to reduce risk ..... 15
Step 7: Sign off and record outcomes ..... 16

# 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?** – SISRA Analytics is a software application which enables Summerhill School to improve their management of pupil assessment data, whilst reducing staff time, paperwork and administration.

SISRA Analytics brings together pupil progress, performance and pastoral data, SISRA Analytics can be used throughout the school year, and not just focusing on exam results analysis. Data is made accessible across Key Stages, it is accessible to all staff, whilst simplifying the management process. Schools can upload quickly and easily from any Management Information System, on any internet-connected device, and give staff access to the information they need through a series of intuitive, easy-to-read reports.

SISRA Analytics allows schools to perform in-depth analysis of pastoral Attitude to Learning (AtL) data alongside pupil grade data, providing staff with greater insight than ever before. SISRA Analytics enables Summerhill School to:

(1) Compare Attitude to Learning (AtL) judgements alongside your grade data to assist with pastoral analysis

(2) Configure up to three AtL categories e.g. Attitude, Behaviour & Organisation. Summerhill School can configure up to three highly customisable AtL categories for analysis of groups, qualifications, classes or individual students. The school can even choose whether aggregated figures are displayed as average judgement, average points or total points

(3) View the impact AtL has on the performance of qualifications, classes and students

(4) Filter by multiple AtL categories across the reports

This functionality enables Summerhill School to track assessment and learning which can all be recorded on the system, in a safe, secure and searchable method.

Summerhill 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 SISRA Analytics the school aims to achieve the following:

1. Management of assessment pupil information in one place
2. Security and integrity of personal data through a secure password protected login.
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. Governors or Ofsted
6. Tracking year groups and identifying trends
7. Ability to add information from Teachers and HLTA's and a small number of TA's across the school
8. Secure access across all devices wherever the setting

The school currently holds the information in hard copy formats. The school recognises that having a manual record has the potential for third party access to personal data or loss of information as a result of fire and flooding. By purchasing an electronic system this goes some way to mitigate against this risk.

Cloud based systems enable the school to upload information to a hosted site to share with others within school. These files can then be accessed securely from any location or any type of device (laptop, mobile phone, tablet, etc).

SISRA Analytics cannot do anything with the school's data unless they have been instructed by the school. The schools Privacy Notice will be updated accordingly.

Summerhill School has included SISRA Analytics 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 lawful basis of why the school collects data. The lawful basis in order to process personal data in line with the 'lawfulness, fairness and transparency principle is as follows:

6.1 (c) Processing is necessary for compliance with a legal obligation to which the controller is subject; e.g. health & safety and safeguarding

6.1 (e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

6.1 (f) Processing is necessary for the purposes of the legitimate interest pursued by the controller or by a third party

The lawful basis for collecting special category information relates to Article 9 2 (g) *processing is necessary for reasons of substantial public interest and is authorised by domestic law.*

The school has considered the lawful basis by which it processes personal data. This is recorded in Summerhill School Privacy Notice (Student) and where appropriate in Privacy Notice (Workforce).

**How will you collect, use, store and delete data?** – SISRA Analytics collects information from the management information system. The information will be stored on SISRA Analytics. The information is retained according to the school's Data Retention Policy.

**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. Assessment are uploaded by staff.

**Will you be sharing data with anyone?** – Summerhill School won't share the data with anyone.

**What types of processing identified as likely high risk are involved?** – The information is transferred securely from the school to the server which is hosted remotely on a server within the UK. Access to information on SISRA Analytics is controlled through passwords, with additional security to the most sensitive information.

**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?** – Full Name of Pupil, UPN, Date of Birth, Registration Group, Gender, Year Group, Pupil Premium, and SEN Types at the very least.

**Special Category data?** – The personal data accessed via the school's management information system will contain special category data as defined by data protection law.

The lawful basis for collecting special category information relates to Article 9 2 (g) *processing is necessary for reasons of substantial public interest and is authorised by domestic law in respect to* The Children Act and subsequent amendments and The Education Act.

SISRA Analytics is not setup to process any special category of data by default, however it is highly customizable. Summerhill School can add and process special category data fields within the service if it wishes to do so with regard to the lawful basis identified above.

**How much data is collected and used and how often?** – 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. It is reviewed termly and updated as necessary.

**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.

**Scope of data obtained?** – How many individuals are affected 1094 and for archived pupils. The geographical area covered is from Year 7 to Year 11 pupils.

**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?** – Summerhill School collects and processes personal data relating to its pupils to ensure the school provides education to its students delivering the National Curriculum.

Through the Privacy Notice (Pupil) Summerhill 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 the software application. SISRA Analytics can restrict access to the designated persons file and restrict access to searching information on the system. Access to the data held on SISRA Analytics will be controlled by username and password.

Access to SISRA Analytics can be revoked at any time. As a default, passwords must be changed every year.

The school will be able to upload personal data from its PC for the data to be stored remotely. Any changes made to files are automatically copied across and immediately accessible from other devices the school may have.

**Do they include children or other vulnerable groups?** – All of the data will relate to children. The information will relate to assessment data including special category data.

**Are there prior concerns over this type of processing or security flaws? –** How is the information stored? Does the cloud provider store the information in an encrypted format? What is the method of file transfer? How secure is the network and what security measures are in place?

Summerhill School recognises that moving from a manual system to an electronic system which holds sensitive personal data in the cloud raises a number of General Data Protection Regulations issues as follows:

- **ISSUE:** SISRA Analytics will be storing personal data
  **RISK:** There is a risk of unauthorized access to information by third parties
  **MITIGATING ACTION:** SISRA Analytics have put in place appropriate security measures to prevent the school's personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, SISRA Analytics limit access to the school's personal data to those employees, agents, contractors and other third parties who have a business need to know.

  SISRA Analytics will only process the school's personal data on SISRA Analytics instructions and they are subject to a duty of confidentiality

- **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 data is encrypted from source and in transit (from the management information system to SISRA Analytics) to the data centre and back again to the data controller

  SISRA Analytics websites uses the latest technology of SSL certificates for encryption of data in transit

- **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:** All data is stored on servers in Birkenhead, UK. This means that the UK GDPR privacy rules apply to the cloud based service

- **ISSUE:** SISRA Analytics as a third party processor and privacy commitments respecting personal data, i.e. the rights of data subjects
  **RISK:** UK GDPR non-compliance
  **MITIGATING ACTION:** It is advisable that the school tailor any contract to incorporate these privacy commitments

- **ISSUE:** Implementing data retention effectively in the cloud
  **RISK:** UK GDPR non-compliance
  **MITIGATING ACTION:** SISRA Analytics will only retain the school's personal data for as long as necessary to fulfil the purposes collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements

  To determine the appropriate retention period for personal data, SISRA Analytics consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which

it processes personal data and whether SISRA Analytics can achieve those purposes through other means, and the applicable legal requirements

In terms of pupil information/performance data *(School decides on the data to be uploaded)*. Staff names & email addresses data is automatically deleted 30 days from expiry/termination of agreement or immediately on written request

- **ISSUE:** Responding to a data breach
  **RISK:** UK GDPR non-compliance
  **MITIGATING ACTION:** SISRA Analytics have put in place procedures to deal with any suspected personal data breach and will notify the school and any applicable regulator of a breach where legally required to do so

- **ISSUE:** Post Brexit
  **RISK:** UK GDPR non-compliance
  **MITIGATING ACTION:** All data is stored on servers in Birkenhead, UK. This means that the UK GDPR privacy rules apply to the cloud based service

  SISRA Analytics will continue to adhere to GDPR rules unless a new regulation is enforced by UK government

- **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:** The Privacy Notice of SISRA Analytics notes the rights of data subjects to have access to their data. In this eventuality SISRA Analytics will provide the technical capability to ensure the school can comply with a data subject access requests. This may be included as part of the contract

- **ISSUE:** 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
  **RISK:** The school is unable to exercise the rights of the individual
  **MITIGATING ACTION:** The Privacy Notice of SISRA Analytics notes the rights of data subjects to have access to their data. In this eventuality SISRA Analytics will provide the

technical capability to ensure the school can comply with a data subject access requests. This may be included as part of the contract

- **ISSUE:** Data Ownership
  **RISK:** UK GDPR non-compliance
  **MITIGATING ACTION:** The school maintains ownership of the data and this should be included in the contract. SISRA Analytics are 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:** SISRA Analytics and SISRA Observe data is kept on a different, isolated domain from all other SISRA data

- **ISSUE:** Data is not backed up
  **RISK:** UK GDPR non-compliance
  **MITIGATING ACTION:** All data is backed up daily in 3 separate locations

  Backups are primarily for disaster recovery in the event of school data becoming lost or corrupted on the live system

- **ISSUE:** UK GDPR Training
  **RISK:** UK GDPR non-compliance
  **MITIGATING ACTION:** Appropriate training is undertaken by personnel that have access to SISRA Analytics

- **ISSUE:** Security of Privacy
  **RISK:** UK GDPR non-compliance
  **MITIGATING ACTION:** SISRA is Cyber Essential certified

**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 for assessment will realise the following benefits:

1. Management of assessment pupil information in one place
2. Security and integrity of personal data through a secure password protected login.
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. Governors or Ofsted
6. Tracking year groups and identifying trends
7. Ability to add information from Teachers and HLTA's and a small number of TA's 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 and the Board of Governors 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:

- The Education Act
- The Childcare Act 2006
- The Children Act

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

SISRA Analytics 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 |
| Subject Access Request | Probable | Significant | Medium |
| Upholding rights of data subject | Probable | Significant | Medium |
| Data Retention | Probable | Significant | Medium |



14

# 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 UK, Cyber Essentials Certified | Reduced | Medium | Yes |
| Data Breaches | Documented in contract and owned by school | 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 | Reduced | Low | Yes |



15

# Step 7: Sign off and record outcomes

| Item | Name/date | Notes |
|---|---|---|
| Measures approved by: | Vicki Poole | Integrate actions back into project plan, with date and responsibility for completion |
| Residual risks approved by: | Vicki Poole | If accepting any residual high risk, consult the ICO before going ahead |
| DPO advice provided: | No | 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)* Transfer of data between the school and the cloud do you offer end to end encryption? *Yes, all our websites uses the latest technology of SSL certificates for encryption of data in transit.*

*(2)* Where is the data stored, i.e. location of servers? *All data is held on our servers in Birkenhead, UK.*

*(3)* If outside the EEA do you use standard contract clauses, with third parties, as approved by the EU. *N/A*

*(4)* In terms of cloud architecture is schools data kept separate from other data, i.e. servers are partitioned? *Yes, SISRA Analytics and SISRA Observe data is kept on a different, isolated domain than all other SISRA data.*

*(5)* What contingency plans have you got in place in terms of a no deal Brexit? *We will continue to adhere to GDPR rules unless a new regulation is enforced by UK government.*

*(6)* Is the data backed up? *Yes, all data is backed up daily in 3 separate locations.*

*(7)* *Does SISRA Analytics have any accreditation/registered with ICO, etc? SISRA is Cyber Essential certified.*

*(8)* Does SISRA Analytics use special category data provided by the school as defined under data protection law? *SISRA Analytics it's not setup to process any special category of data by default, however it's highly customizable. Users could potentially add and process special category data fields within the service if they wish to do so.*

| | | |
|---|---|---|
| DPO advice accepted or overruled by: N/A<br>If overruled, you must explain your reasons | | |
| Comments: | | |
| Consultation responses reviewed by:<br>If your decision departs from individuals' views, you must explain your reasons | | |
| Comments: | | |
| This DPIA will kept under review by: | Vicki Poole | The DPO should also review ongoing compliance with DPIA |



17