

STUART BATHURST CATHOLIC HIGH SCHOOL



Data Protection Impact Assessment (SISRA ANALYTICS)

Data Protection Impact Assessment (SISRA Analytics)

Stuart Bathurst Catholic High 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 Stuart Bathurst Catholic High 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. Stuart Bathurst Catholic High School recognises that using a cloud-based system has a number of implications Stuart Bathurst Catholic High 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 considering 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.

Stuart Bathurst Catholic High School aims to undertake a review of this Data Protection Impact Assessment on an annual basis.

What is the aim of the project?

SISRA Analytics is a software application which enables Stuart Bathurst Catholic High 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 Stuart Bathurst Catholic High School to:

- Compare Attitude to Learning (AtL) judgements alongside your grade data to assist with pastoral analysis
- Configure up to three AtL categories e.g. Attitude, Behaviour & Organisation. Stuart Bathurst Catholic High 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
- View the impact AtL has on the performance of qualifications, classes and students
- Filter by multiple AtL categories across the reports

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

Stuart Bathurst Catholic High School will undertake the following processes:

- Collecting personal data
- Recording and organizing personal data
- Storing personal data
- Copying personal data
- Retrieving personal data
- Deleting personal data

By opting for SISRA Analytics the school aims to achieve the following:

- Management of assessment pupil information in one place
- Security and integrity of personal data through a secure password protected login.
- Storage of information electronically rather than manually
- Recording information and building a chronology around the pupil
- Providing bespoke reports for different audiences, e.g. Governors or Ofsted
- Tracking year groups and identifying trends
- Ability to add information from Teachers and HLTA's and a small number of TA's across the school
- Secure access across all devices wherever the setting

The school currently holds the information in hard copy formats. These are kept securely in a locked cabinet behind a locked door in the Headteachers office. 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 school's Privacy Notice will be updated accordingly.

Stuart Bathurst Catholic High School has included SISRA Analytics within its Information Asset Register.

The Privacy Notices (pupil) for the school provides the legitimate basis of why the school collects pupil data. Specifically, this relates to The Children Act and subsequent amendments, The Education Act and subsequent amendments and The Childcare Act 2006

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?

Stuart Bathurst Catholic High 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.

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 this information relates to Article 9 2 (b) *processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject 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. Stuart Bathurst Catholic High 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.

What is the nature of your relationship with the individuals?

Stuart Bathurst Catholic High 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) Stuart Bathurst Catholic High 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.

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.

Stuart Bathurst Catholic High 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 request. 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 request. 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

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

- Management of assessment pupil information in one place
- Security and integrity of personal data through a secure password protected login.
- Storage of information electronically rather than manually
- Recording information and building a chronology around the pupil
- Providing bespoke reports for different audiences, e.g. Governors or Ofsted
- Tracking year groups and identifying trends
- Ability to add information from Teachers and HLTA's and a small number of TA's across the school
- Secure access across all devices wherever the setting

The views of senior leadership team and the Board of Governors will be obtained. Once reviewed the views of stakeholders will be considered.

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

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.

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

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
Data Transfer	Secure network, end to end encryption	Eliminated reduced accepted Reduced	Low medium high Medium	Yes/no 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

Item	Name/date	Notes
Measures approved by:	Richard May	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Richard May	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
<p>Summary of DPO advice: Technical recommendations to be clarified with third party as follows:</p> <p>Transfer of data between the school and the cloud do you offer end to end encryption? <i>Yes, all our websites uses the latest technology of SSL certificates for encryption of data in transit.</i></p> <p>Where is the data stored, i.e. location of servers? <i>All data is held on our servers in Birkenhead, UK.</i></p> <p>If outside the EEA do you use standard contract clauses, with third parties, as approved by the EU. <i>N/A</i></p> <p>In terms of cloud architecture is schools data kept separate from other data, i.e. servers are partitioned? <i>Yes, SISRA Analytics and SISRA Observe data is kept on a different, isolated domain than all other SISRA data.</i></p> <p>What contingency plans have you got in place in terms of a no deal Brexit? <i>We will continue to adhere to GDPR rules unless a new regulation is enforced by UK government.</i></p> <p>Is the data backed up? <i>Yes, all data is backed up daily in 3 separate locations.</i></p> <p><i>Does SISRA Analytics have any accreditation/registered with ICO, etc? SISRA is Cyber Essential certified.</i></p> <p><i>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.</i></p>		
<p>DPO advice accepted or overruled by:</p> <p>If overruled, you must explain your reasons</p>		
<p>Comments:</p>		
<p>Consultation responses reviewed by:</p> <p>If your decision departs from individuals' views, you must explain your reasons</p>		
<p>Comments:</p>		
This DPIA will kept under review by:	Alicia Mortimer	The DPO should also review ongoing compliance with DPIA