STUART BATHURST CATHOLIC HIGH SCHOOL

Data Protection Impact Assessment (Provision Map)

Data Protection Impact Assessment (Provision Map)

Stuart Bathurst Catholic High School operates a cloud-based system or 'hosted solution', called Provision Map. Access to Provision Map is through the internet. Resources are retrieved from Provision Map via the Internet, through a web-based application, as opposed to a direct connection to a server at the school. Access to Provision Map is through a web browser. As 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 'hosted solution' 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 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.

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?

Stuart Bathurst Catholic High School operates a manual system. Information is located within a locked cabinet within the school building. The hard copy information comprises of provision maps which are produced using Microsoft Office and stored in the secure area (SENCo folder) of the schools' network for pupils enrolled at Stuart Bathurst Catholic High School. The provision maps are printed and shared with the relevant class teacher which are stored in locked cupboards in the classroom.

Teachers and Teaching Assistants only have access to the relevant pupil files for their class, access to all these files is restricted to the Headteacher and the SENCo. Hard copy documents are sent to the receiving school at the end of Year 6 and electronic copies are deleted from the SENCo folder on the network in line with the school's data retention policy.

Provision Map is a hosted system which means that all updates, maintenance and management can be performed in a central location by Edukey Education Limited.

Provision Map enables Stuart Bathurst Catholic High School to improve their management of child special educational needs, whilst reducing staff time, paperwork and administration.

Specifically, it maps out SEN interventions helping professionals keep track with the pupil and staff involved in each intervention. It integrates SEN management cycle with automatic review reminders. Provision map generates cost, time, pupil premium and outcome reports in an instant. The outcome tracking feature makes it easier for the school to see the impact of the interventions and plans in place and for the school to act accordingly.

Provision Map is an intuitive system to help with the management and recording of child special educational needs. Provision Map allows the recording in one place sensitive information within an electronic format which is held securely on a remote server.

Provision Map enables Stuart Bathurst Catholic High School to centralise the data, share information with parents and carers by improving the level of granularity of data and relevant agencies. A meeting held with relevant parties can all be recorded on the system, in a safe, secure and searchable method. Recording sensitive pupil information electronically is password protected which will help mitigate against the risk of a data breach with the appropriate controls in place.

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 Provision Map the school aims to achieve the following:

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

The school currently holds the information in a hard copy format. This is kept securely in a locked cabinet within a locked room. The school recognizes that having a manual record has the potential for third party access to sensitive 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 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.

Provision Map 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 Provision Map is the data processor.

Stuart Bathurst Catholic High School has included Provision Map 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 health and safety and safeguarding of vulnerable groups. Provision Map is referenced in the respective Privacy Notices.

How will you collect, use, store and delete data?

Provision Map collects information from pupil records, Special Educational Needs (SEN) records, Education Health Care Plans (EHCP). Provision Map links into Stuart Bathurst Catholic High School Management Information System drawing pupil data into the application. The information will be stored on Provision Map. 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. SENCO records, Education Health and Care Plans, Pupil Records, and Early Help Assessment.

Provision Map collects personal data from the school's management information system which is RM Integris.

Will you be sharing data with anyone?

Stuart Bathurst Catholic High School may share information with SEND professionals including the SENCo, Headteacher, Senior Leadership Team (SLT), Governors, Ofsted, the local authority, i.e. Educational Psychologist, Occupational Therapist and Speech and Language Therapist. However, this does not mean that Stuart Bathurst Catholic High School shares Provision Map 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.

What is the nature of the data?

Pupil data relates to personal identifiers and contacts (such as name, unique pupil number, contact details and address). Characteristics (such as ethnicity, language, nationality, gender, religion, data of birth, country of birth, free school meal eligibility). Names of other agencies involved, i.e. speech and language therapists, occupational therapist, educational psychologist, and details of outcomes.

Provision Map contains electronic records of the work of the School in identifying SEND needs, monitoring progress and outcomes. It also includes safeguarding information, medical and administration (doctors' information, child health, dental health, allergies, medication and dietary

requirements). Attendance information, assessment, attainment and behavioral information. The school also obtains data on parents/guardians/carers including their name, address, telephone number and e-mail address.

Workforce data relates to personal information (such as name, address and contact details, employee or teacher number, salary, bank details, national insurance number, marital status, next of kin, dependents and emergency contacts). Special categories of data (such as gender, age, ethnic group). In particular, salary data is collected to enable the school to calculate the cost of interventions.

Special Category data?

Data revealing racial or ethnic origin, medical details are collected by the school and contained in Provision Map. 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. Provision Map also has the facility for a direct transfer of data held in its system to a receiving school as long as they have the same product. This retention period has also been agreed in consultation with the Safeguarding Children Board on the understanding that the principal copy of this information will be found on the Local Authority Social Services record.

Scope of data obtained?

Data will relate to pupils at Stuart Bathurst Catholic High School

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 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 reports, trends and profiling produced by Provision Map.

Through the Privacy Notice (Pupil) and (Workforce) 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 SEND information. Provision Map can restrict access so that only designated staff only see information that is relevant to them. Access to the data held on Provision Map will be controlled by username and password.

Additionally, whilst Provision Map works on any device with access to the internet, staff that are granted access to the system will have to utilise an additional password to their own, which is only shared between authorized members of staff at the school. Individuals working for third-party agencies are sent an invitation by the SENCo officer to access the system.

The school will be able to upload personal data from its PC for the data to be stored remotely, such as EHCPs. 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 SEND, health plans, pupil attendance and assessment, etc.

Are there prior concerns over this type of processing or security flaws?

All data is secured in transit using 256 bit SSL encryption. It is securely stored at rest within industry leading data storage standards.

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 UK General Data Protection Regulations issues as follows:

ISSUE: Provision Map will be storing personal data
RISK: There is a risk of unauthorized access to information by third parties
MITIGATING ACTION: Edukey Education Ltd school data is stored on approved and compliant cloud infrastructure. Access to all parts of the infrastructure is available to Edukey Education Ltd 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 user-names and passwords

Security-centred code reviews and testing is performed on all newly developed features. Regular vulnerability scanning is performed using in-house and independent (supplied by Detectify) automated vulnerability scanners

Security related updates for all software used across the infrastructure is installed in a timely manner. Dual factor authentication is enforced for all Edukey staff and for all services used in relation to the product

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 Provision Map 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 Provision Map server is the server it says it is. Connections are encrypted with 256-bit AES encryption. AES encryption is a US government standard for encryption, and 256-bit is the highest level available. SSL encryption takes place between the school's computer and the Provision Map server when accessing Provision Map and between the school's Management Information System (MIS) and the Provision server when school data is being transferred through an automatic extract

In addition to the SSL encryption, which ensures data transfer between the school's computer and the Provision Map server, and the school's MIS and the Provision Map server, is encrypted, Provision Map also perform data encryption on any sensitive information stored in the Provision Map databases

The text of incidents, actions, and documents are encrypted when they are stored and unencrypted when an authenticated request is made to view them. This means if unauthorised access was obtained to the database where the information is stored, the data would still be encrypted and be unable to be viewed. This encryption also takes place using 256-bit AES encryption

All staff who work on Provision Map are employed by EduKey Education Limited directly and are fully DBS checked

ISSUE: Understanding the cloud-based solution chosen where data processing/storage premises are shared?
RISK: The potential of information leakage
MITIGATING ACTION: Edukey Education Ltd's servers are hosted by Google Cloud and Rackspace in London, UK. The data centre is staffed by a team of highly trained, on-site engineers and security experts who work around the clock to ensure that the systems are secure and running strong. Data centres have built in multiple layers of redundancy, at every level - including physical security, power, cooling and networks. These redundancies help make the data centre more resilient and reliable

Rackspace is restricted by biometric authentication, keycards and 24 x 7 x 365 surveillance. These ensure that only authorised engineers have access to routers, switches and servers. Google Cloud data centres incorporate multiple layers of physical security protections. Access to these data centres is limited to only a very small fraction of Google employees. They use multiple physical security layers to protect our data centre floors and use technologies like biometric identification, metal detection, cameras, vehicle barriers, and laser-based intrusion detection systems

Edukey Education Ltd back-up nightly and retain the last fourteen back-ups. Backups are managed by data centres and are redundant. They are in the same physical location (London) but on completely different servers

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: Edukey Education Ltd servers are hosted by Google Cloud and Rackspace in the UK to ensure school data is retained within the European Economic Area

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 Edukey Education Ltd support technical staff can access it. Edukey Education Ltd staff are vetted and are subject to contractual data access policies and confidentiality clauses. DBS checking is carried out on all staff

User access is based on individual usernames and passwords. User passwords must be a minimum of eight characters long and contain at least one number and one capital letter. Users have eight

log-in attempts before they are locked out. Additional levels of security can be added such as locking access to the school IP address so that users need to be on site to gain access. Edukey Education Ltd commits to restrict access to customer data only to those individuals who require such access to perform their job function

ISSUE: Implementing data retention effectively in the cloud
RISK: UK GDPR non-compliance
MITIGATING ACTION: Edukey Education Ltd will delete all data 30 days after closing the school's account. The data will be completely eradicated fourteen days later from the company's backups. If a school cancels their contract with Edukey Education Ltd then their account is set into 'Awaiting Deletion' state. Deletion then occurs automatically within 30 days. Data remains in encrypted backups until the 30-day cycle is complete. All deletion of data and deletion of backup files are logged

Edukey Education Ltd can either provide, or will provide, means for authorised client users to implement data retention activities directly

ISSUE: Responding to a data breach
RISK: UK GDPR non-compliance
MITIGATING ACTION: Edukey has policies and procedures in place to ensure school's are notified in the event of data breaches as required by UK GDPR. Edukey Eduction Ltd has e-mail notifications for failed login attempts to any of their resources. Edukey blocks users after a certain number of invalid login attempts within a time window. Edukey Education Ltd uses error log monitoring software (Loggly) to alert the company to unusual activity

If the school becomes aware of a breach it will contact the dedicated Edukey Education Ltd account administrator 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: Edukey Education Ltd back-up nightly and retain the last fourteen back-ups. Backups are managed by Rackspace/Google Cloud and are redundant. They are in the same physical location (London) but on completely different servers. In terms of disaster recovery, the restore process is managed by Edukey Education Ltd within 24 hours. In terms of business continuity key staff have responsibilities to ensure critical business activities are prioritised and restored. Non-critical activities are suspended and essential resources are focused to support critical ones. These are recovered when all critical activities have been resumed.

ISSUE: Post Brexit
RISK: UK GDPR non-compliance
MITIGATING ACTION: Provision Map servers are hosted in the UK

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: Provision Map 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 Edukey Education Ltd 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. Provision Map 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: Edukey Education Ltd use multiple protective layers with the cloud platform to protect its services. These include encryption and firewalling. The company carry out routinely vulnerability and penetration testing and promptly address any issues identified. This should be monitored to address any changes in technology and its impact on data. The school should maintain ownership of the Cloud technologies used ensuring the current and future technologies enable UK GDPR compliance

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

ISSUE: Security of Privacy
RISK: UK GDPR non-compliance
MITIGATING ACTION: Edukey Education Ltd hold Cyber Essentials Certification - Certificate Number: IASME-A-07641. ICO registration number Z1932768. Google Cloud and Rackspace data centres are certified to the international standard for information security, ISO27001. Edukey Education Ltd meets Cyber Essentials for cyber protection

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

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

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

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.

Provision Map 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
	Possible	Severe	Medium
Data transfer; data could be compromised	Possible	Significant	Medium
Asset protection and resilience	Possible	Significant	Medium
Data Breaches	Probable	Significant	Medium
	Probable	Significant	Medium
Subject Access Request	Probable	Significant	Medium
Upholding rights of data subject			
Data Retention			

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 Asset protection & resilience Data Breaches Subject Access Request Upholding rights of data subject Data Retention	Secure network, end to end encryption Data Centre in UK, Cyber Essentials Certification Documented in contract and owned by school Technical capability to satisfy data subject access request Technical capability to satisfy rights of data subject Implementing school data retention periods as outlined in the IRMS Information Management Toolkit for Schools and data retention policy	Eliminated reduced accepted Reduced Reduced Reduced Reduced Reduced	Low medium high Medium Medium Low Low Low Low	Yes/no Yes Yes Yes Yes Yes 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
Summary of DPO advice: Technical recommendations to be clarified with third party as follows: Does Provision Map 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?)* 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)* What certification does Provision Map have?, *(e.g. ISO 27001 certified, ICO registration)*		
DPO advice accepted or overruled by: If overruled, you must explain your reasons		
Comments:		
Consultation responses reviewed by: If your decision departs from individuals' views, you must explain your reasons		
Comments:		
This DPIA will kept under review by:	Alicia Mortimer	The DPO should also review ongoing compliance with DPIA