STUART BATHURST CATHOLIC HIGH SCHOOL

Data Protection Impact Assessment (Class Charts)

Data Protection Impact Assessment (Class Charts)

Stuart Bathurst Catholic High School operates a cloud-based system or 'hosted solution', called Class Charts. Access to Class Charts is through the internet. Information is retrieved from Class Charts via the Internet, through a web-based application, as opposed to a direct connection to a server at the school. Access to Class Charts is through a web browser. 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 '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 previously operated a manual house merit point based system which was based on information obtained from SIMS.net.

All teaching staff will have access to the system, including a limited number of support staff. Access is dependent on job role and need. Class Charts provides a level of access to facilitate this requirement.

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

Class Charts enables Stuart Bathurst Catholic High School to improve their behaviour management system where there are a series of reward management / escalations depending upon the nature of the issue reported, whilst reducing staff time, paperwork and administration. The behaviour management system includes the recording of positive and negative events.

Class Charts provides a dashboard facility where students who have received positive and negative awards are displayed in an easy-to-view manner which helps the school to identify any concerns or actions quickly. This feature makes it easier for the school to apply interventions and have plans in place for the school to act accordingly.

Class Charts also provides a facility to record attendance which is linked to a class seating plan. The seating plan can be automatically generated based on a number of factors which the member of staff has full control over. In addition, based on student's behaviour information, the seating plan can be generated by the Class Charts system. At all stages of the presentation of the seating plan, the teacher will review and approve the plan using their knowledge of individual students and their background.

Reports can be generated based on tutor or class groups, daily activities and attendance. Class Charts also provides a further granular facility to extract and report on information.

Class Charts does not extract or display parental contact data, therefore SIMS.net will still be used for contacting parents when following up on events recorded via Class Charts.

Stuart Bathurst Catholic High 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 Class Charts 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

Where the school had a previous manual process to record behavior event information, it recognised 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.

Class Charts 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 Class Charts is the data processor.

Stuart Bathurst Catholic High School has included Class Charts within its Information Asset Register.

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

Class Charts collects information from pupil records, Special Educational Needs (SEN) records and behavior records. Class Charts links into Stuart Bathurst Catholic High School Management Information System drawing pupil data into the application via the Wonde data extraction service. The information will be stored in Class Charts. 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.

Class Charts collects personal data from the school's management information system which is Capita SIMS.net.

Will you be sharing data with anyone?

Stuart Bathurst Catholic High School may share information with education professionals including the SENCo, Headteacher, Senior Leadership Team (SLT), Governors, Ofsted, the local authority. Parents also have access to their child's information through the Class Charts portal. However, this does not mean that Stuart Bathurst Catholic High School shares Class Charts 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, tutor, teaching group membership). Characteristics (such as free school meal eligibility). Only a limited amount of information is displayed in Class Charts, which includes name, class group, free school meals entitlement and SEND. These last two pieces of information are only identified using symbols or icons in the class group screen.

Workforce data relates to personal information (such as name, tutor group(s) and teaching groups. 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 Class Charts. 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 (approximately 1012 for safeguarding issues and concerns) and for pastoral issues (approximately 1012 pupils). The geographical area covered is from pupils aged 11 (Year 7) to age 16 (Year 11).

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 with the creation of login accounts dependent on job role.

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 Class Charts. The school can use Class Charts can restrict access so that only designated staff only see information that is relevant to them. Access to the data held on Class Charts will be controlled by username and password.

Additionally, whilst Class Charts 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. Staff utilise iPads or their classroom workstation to access the facility. Access to the system is during normal working hours in order that the system can be updated 'live'.

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.

What other features does the system have?

Class Charts has a facility to 'write back' information gathered through the system, to SIMS.net. This improves the efficiency of the data gathered so that if a report is required from SIMS.net, accurate and up to date information is available.

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 General Data Protection Regulations issues as follows:

- **ISSUE:** Class Charts 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 Class Charts 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 Class Charts 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 Class Charts server when accessing Class Charts 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 Class Charts server, and the school's MIS and the Class Charts server, is encrypted, Class Charts also perform data encryption on any sensitive information stored in the Class Charts 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 Class Charts 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 schools 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: Class Charts 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: Class Charts 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

Under the circumstance of any of the above, the data subject is requested to email support@edukey.co.uk and they will assist or provide the relevant steps where necessary

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: As Data Controller the school maintains ownership of the data. Class Charts 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 UK GDPR Training
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Appropriate training is undertaken by personnel that have access to Class Charts

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Edukey Education Ltd hold Cyber Essentials Certification - Certificate Number: IASME-CE-015504. ICO registration number is 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:

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

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

Class Charts 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

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 Upholding rights of data subject	Technical capability to satisfy data subject access request	Reduced	Low	Yes
Data Retention	Technical capability to satisfy rights of data subject	Reduced	Low	Yes
	Implementing school data retention periods as outlined in the IRMS Information Management Toolkit for Schools and data retention policy	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

Summary of DPO advice: Technical recommendations to be clarified with third party as follows:

(1) Does Class Charts 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?)*

Answer provided Under the circumstance of any of the above, please email support@edukey.co.uk and we will assist or provide the relevant steps where necessary.

(2) 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 & multi factor access control systems)*

Answer provided: https://www.edukey.co.uk/wp-content/uploads/GDPR_Summary.pdf

(3) 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)*

Answer provided: For Class Charts we request that record deletion requests are emailed to support@edukey.co.uk. We have introduced user functionality for this in Provision Map, and may introduce the ability for Class Charts in the future. Additionally, all data is deleted 30 days after license termination

(4) What certification does Class Charts have? *(e.g. ISO 27001 certified, ICO registration)*

Answer provided: We are registered with the ICO under 'Tes Global Limited', and have a Cyber Essentials registration - Certificate number: IASME-CE-015504.

DPO advice accepted or overruled by: No 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