Data Protection Impact Assessment (CPOMS)

St. Mark's Catholic Primary School operates a cloud based system or 'hosted solution', called CPOMS. Access to CPOMS is through the internet. Resources are retrieved from CPOMS via the Internet, through a web-based application, as opposed to a direct connection to a server at the school. Access to CPOMS can be through a PC, smartphone, iPad and tablet. As such St. Mark's Catholic Primary 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. St. Mark's Catholic Primary School recognises that using a 'hosted solution' has a number of implications. St. Mark's Catholic Primary 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. St. Mark's Catholic Primary 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.

1

Contents

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? – St. Mark's Catholic Primary School operates a manual system. Information is located within a locked cabinet within a locked room in three locations within the school building. The hard copy information comprises of behavior issues, Special Education Needs (SEN) records, safeguarding and pastoral information including potential Child Protection issues for pupils enrolled at St. Mark's Catholic Primary School. Some of the personal data relates to information relating to former pupils where the school has yet to identify where the pupil has been transferred to. Access to these files is restricted to the Headteacher and the Designated Safeguarding Lead (DSL).

CPOMS is a hosted system which means that all updates, maintenance and management can be performed in a central location by CPOMS Systems Limited. It is hosted in secure UK data centres, currently in Berkshire and South Yorkshire, with 24 hour security including full CCTV coverage.

CPOMS enables St. Mark's Catholic Primary School to improve their management of child protection and similar incidents and actions, whilst reducing staff time, paperwork and administration.

CPOMS is an intuitive system to help with the management and recording of child protection, behavioural issues, bullying, special educational needs, domestic issues and more. CPOMS contains sensitive information within an electronic format which is held securely on a remote server.

CPOMS also enables the school to track referrals to external agencies, such as NHS/CAHMS, Children's Services, and the Police (including letters and phone calls) and to be alerted if timescales are not being met.

This same functionality enables St. Mark's Catholic Primary School to track communication with parents and carers, as well as the students themselves. A meeting held, conversation with a child, or a decision to undertake an Early Help Assessment can all be recorded on the system, in a safe, secure and searchable method.

3

To record sensitive pupil information electronically which is password protected will help mitigate against the risk of a data breach with the appropriate controls in place.

CPOMS has a Privacy Notice which states that for the purposes of IT hosting the information may be located on servers within the European Union.

St. Mark's Catholic Primary 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 CPOMS 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. Alerting staff and setting up reminders as appropriate
6. Providing bespoke reports for difference audiences, e.g. Governors or Ofsted
7. Tracking vulnerable groups and identifying trends
8. Ability to add information from staff across the school
9. 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.

4

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 any location or any type of device (laptop, mobile phone, tablet, etc).
CPOMS 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 CPOMS is the data processor.

St. Mark's Catholic Primary School has included CPOMS within its Information Asset Register.

Step 2: Describe the processing

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

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

How will you collect, use, store and delete data? – CPOMS collects information from behavior and attendance records, Special Educational Needs (SEN) records, Education Health Care Plans (EHCP), Safeguarding records and from other sources. CPOMS links into St. Mark's Catholic Primary School Management Information System drawing pupil data into the application. The information will be stored on CPOMS. The information is retained according to the school's Data Retention Policy.

What is the source of the data? – Attendance and behavior information, Safeguarding files, SENCO records, Education Health and Care Plans, Pupil Records, and Early Help Assessment.

Will you be sharing data with anyone? – St. Mark's Catholic Primary School may share information with safeguarding professionals including the Designated Safeguarding Lead,

SENCO, headteacher, Senior Leadership Team (SLT), Governors, Ofsted, the local authority, i.e. Safeguarding Children Board, Local Authority Designated Officer (LADO), Social Services, the NHS/CAHMS, the Police, according to agreed safeguarding procedures. However, this does not mean that St. Mark's Catholic Primary School shares CPOMS access to the third parties.

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 European Union. Access to information on CPOMS is controlled through passwords, with additional security to the most sensitive information. For example, the Designated Safeguarding Leads and Headteacher would have access to the most sensitive information using a two tiered log in procedure. Other members of staff would only have access to report incidents on CPOMS.

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

What is the nature of the data? – Pupil data relates to the name of the child, date of birth, and class. Data also includes attendance and behavior information and SEN. Names of other agencies involved, i.e. NHS/CAHMS, counselling, early help, speech and language therapists, health visitors, social workers, and details of outcomes. CPOMS contains electronic records of the work of the School in dealing with a suspected/actual safeguarding issue and monitor progress and outcomes.

Special Category data? – Data revealing racial or ethnic origin, and religious beliefs are collected by the school and contained in CPOMS. 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.*

How much data is collected and used and how often? – Personal details relating to pupils are obtained from parent/pupil information systems. Safeguarding content obtained from

6

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.

Safeguarding 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 + 25 years then reviewed. 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? – How many individuals are affected (approximately 210 pupils for safeguarding issues and concerns). The geographical area covered is from Reception to Year 6 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? – St. Mark's Catholic Primary 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.

Through the Privacy Notice (Pupil) St. Mark's Catholic Primary 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 safeguarding information. CPOMS can restrict access to the designated persons file and restrict access to

7

searching information on the system. Access to the data held on CPOMS will be controlled by username and password.

Additionally whilst CPOMS works on any device with access to the internet, those members of staff with higher levels of access to sensitive information must download the CPOMS Authenticator App which provides additional security with access to additional sensitive information. For the password to be accepted, an alphanumeric combination with special characters must be used for the system to accept. It also has the functionality to have an automatic time out facility set by the St. Mark's Catholic Primary School.

Access to CPOMS can be revoked at any time. If a member of staff hasn't logged in, in excess of 60 days, the login will need to be reactivated and a new password set. As a default, passwords must be changed every 60 days.

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 safeguarding, health plans, pupil attendance and behavior, etc.

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?

St. Mark's Catholic Primary 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:** CPOMS will be storing personal data
  RISK: There is a risk of unauthorized access to information by third parties
  MITIGATING ACTION: CPOMS has an enterprise level permissions system which allows each school to uniquely control which members of staff can access each type of

8

sensitive information. Access to view incidents logged inside CPOMS is restricted by "dual factor authentication"

CPOMS' dual factor authentication mechanism requires not only a username and password, but also a 'Soft Key' (using the CPOMS Authenticator App on their mobile phone/ tablet device), which is uniquely associated to each CPOMS users account to access the system

Whenever someone tries to access CPOMS they must provide their username, password and the unique 6-digit passcode, at that moment in time, from their own CPOMS Authenticator App. The 6-digit passcode is ever changing (every 30 seconds) and will only work alongside the account credentials provided – both email address and password. If the 'CPOMS Authenticator App' cannot be used, physical USB keys are available on request

CPOMS permissions are configurable by an authorised admin user at the school and they can be changed and updated at any time by the school, including completely revoking access for users. CPOMS further assist schools in protecting access to the data by having a strong password policy which is automatically enforced. CPOMS has an automatic log out facility and a full audit trail which details user activity within the system

- **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 CPOMS 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 CPOMS 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 CPOMS server when accessing CPOMS and between the school's Management Information

9

System (MIS) and the CPOMS 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 CPOMS server, and the school's MIS and the CPOMS server, is encrypted, CPOMS also perform data encryption on any sensitive information stored in the CPOMS 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

Access to customer data is strictly restricted to only those individuals who require such access to perform their job function. All staff who work on CPOMS are employed by CPOMS Systems 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: CPOMS are partnered with Memset (http://www.memset.com), a specialised UK hosting company who provide data centres. Memset are also an ISO 9001 (Quality) and ISO27001 (Information Security) certified company. Memset use two UK data centres (both in Reading) which are manned 24/7 by dedicated security personnel, with restricted access and internal CCTV monitoring. Using two data centres allows CPOMS hosting service to be resilient.

- **ISSUE:** Cloud solution and the geographical location of where the data is stored

10

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: Data centres are in the UK (owned by Memset) and EEA. This means that the UK GDPR privacy rules apply to the cloud based service

- **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: User permissions within CPOMS ensure that schools are able to fully comply with their obligations with regard to the exercise of data subjects' rights

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: At the end of the contract all data will be returned to the school via password protected encrypted media. Password details will be forwarded by separate secure communication. Once the customer has provided us with written confirmation that they have successfully accessed that data we will arrange for CPOMS copies of school data to be securely deleted from the CPOMS database within 30 days

  Where such data resides on an active SQL database server CPOMS are able to assure the school that their data has been deleted following the above process. Where CPOMS Cloud Services partner Memset have taken SQL database servers out of service (end of life) CPOMS receive a specific assurance from Memset that data on all such servers has been deleted and the media destroyed in line with UK regulations

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The school will recognize the need to define in their contract a breach event and procedures for notifying the school and the school managing it

- **ISSUE:** Data is not backed up
  RISK: UK GDPR non-compliance

11

MITIGATING ACTION: Data is backed up to multiple locations to enable CPOMS to provide maximum resilience. CPOMS Systems Limited has taken a conscious decision to exceed the requirements of the Data Protection Act in this regard in that all schools' data is held within UK Data Centres – it does not move out to the EEA

CPOMS carries out additional daily backups from Memset to our own servers at our data centre in South Yorkshire. In the event of any catastrophic error involving both data centres, this would allow CPOMS to restore service to CPOMS quickly and with no data loss

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Data is stored in 2 primary UK Government accredited Tier 3 secure Data Centres, with backups as standard in 2 separate secure data centres. All CPOMS data is stored and processed not only within the EEA, but entirely within 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: User permissions within CPOMS ensure that schools are able to fully comply with their obligations with regard to the exercise of data subjects' rights

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: As Data Controller the school maintains ownership of the data. CPOMS 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: Data is stored in 2 primary UK Government accredited Tier 3 secure Data Centres, with backups as standard in 2 separate secure data centres. All CPOMS data is stored and processed not only within the EEA, but entirely within the UK

12

As part of ISO27001 accreditation CPOMS Systems Limited (CPOMS) has full Disaster Recovery and Business Continuity plans in place. In addition CPOMS Data Centre architecture includes in built load balancing, automated backups and redundancy in terms of server and network capacity

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

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: CPOMS Systems Limited (CPOMS) is an accredited ISO27001 and G Cloud supplier. As part of that accreditation, CPOMS have annual penetration/vulnerability test performed by a trusted 3rd party partner. In addition to these tests CPOMS Systems Limited (CPOMS) uses a UK based Data Centre supplier who is also accredited to ISO27001 and thus subject to the same security audits. CPOMS is accredited to the latest version of the ISO27001 standard (2013)

  Accreditation requires annual external audits by the accreditation providers and regular internal audits by the senior management including persons at Director level

  CPOMS is ISO 9001. CPOMS holds the Cyber Essentials certification (Cert no 5879434651924013)

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

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

1. Management of sensitive pupil in one place
2. Security and integrity of sensitive data through a secure document vault
3. Storage of information electronically rather than manually

13

4. Recording information and building a chronology around the pupil
5. Alerting staff and setting up reminders as appropriate
6. Providing bespoke reports for difference audiences, e.g. Governors or Ofsted
7. Tracking vulnerable groups and identifying trends
8. Ability to add information from staff across the school
9. 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:

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

14

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

CPOMS 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.

15

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

16

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, Certified, ISO 27001	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

17

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Danielle Linley	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Danielle Linley	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)* How is the information stored on the server? *(e.g. is the server shared with other schools, what security is in place to maintain the integrity of the school's data?)* *(2)* Where is the server located? (3) Do you store the information in an encrypted format? *(if not how is info stored?)* (4) What is the method of file transfer from school to the remote server and vice versa? (5) How secure is the network? *(The school wishes to mitigate against the risk of compromise or unlawful access when personal data is transferred)* (6) What security measures are in place? *(firewalls, etc?)* (7) What certification does CPOMS have?, *(e.g. ISO 27001 certified, etc)*		
DPO advice accepted or overruled by: If overruled, you must explain your reasons		
Comments:		
Consultation responses reviewed by: Danielle Linley If your decision departs from individuals' views, you must explain your reasons		
Comments:		
This DPIA will kept under review by:	Shugufta Hussain	The DPO should also review ongoing compliance with DPIA

18