Data Protection Impact Assessment (SIMS)

St. Mark's Catholic Primary School operates a server based system for storage and access to pupil details and records. 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 this service provider 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 using this MIS 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 data is important to determine applicable law. The school will need to satisfy its responsibilities in determining whether the security measures the 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 this Data Protection Impact Assessment on an annual basis.

A Data Protection Impact Assessment will typically consist of the following key steps:

1. Identify the need for a DPIA.
2. Describe the information flow.
3. Identify data protection and related risks.
4. Identify data protection solutions to reduce or eliminate the risks.
5. Sign off the outcomes of the DPIA.

Contents

Step 1: Identify the need for a DPIA 3

Step 2: Describe the processing 4

Step 3: Consultation process 11

Step 4: Assess necessity and proportionality 11

Step 5: Identify and assess risks 13

Step 6: Identify measures to reduce risk 14

Step 7: Sign off and record outcomes 15

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? – To help deliver a cost effective solution to meet the needs of the business.

St. Mark's Catholic Primary School will undertake the following processes:

1. Collecting personal data
2. Recording and organizing personal data
3. Structuring and storing personal data
4. Copying personal data
5. Retrieving personal data
6. Deleting personal data

By opting for an internal server based solution the school aims to achieve the following:

1. Reliability
2. Resilience
3. Update of documents in real time
4. Good working practice, i.e. secure access to sensitive files

SIMS Server based system enables the school to save documents, photos and other files and to act as a backup copy.

Capita SIMS offers two solutions for schools to utilize the product;

1. an on premise system where the school manages the server itself onsite,
2. or the SIMS hosted (cloud based) system where the school accesses the management information system via a web browser or app and the schools management information data is stored remotely in a data centre.

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 and workforce) for the school provides the legitimate basis of why the school collects data.

How will you collect, use, store and delete data? – The information collected by the school is retained on the school's computer systems and in paper files. 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. Workforce information is collected through application forms, CVs or resumes; information obtained from identity documents, forms completed at the start of employment, correspondence, interviews, meetings and assessments.

Will you be sharing data with anyone? – St. Mark's Catholic Primary School routinely shares pupil information with relevant staff within the school, schools that the pupil attends after leaving, the Local Authority, the Department for Education, Health Services, Learning Support Services, SIMS and various third party Information Society Services applications.

St. Mark's Catholic Primary School routinely shares workforce information internally with people responsible for HR and recruitment (including payroll), senior staff, with the Local Authority, and the Department for Education.

What types of processing identified as likely high risk are involved? – Transferring 'special category' data from the school to local authority, and to hosted servers remotely. Storage of personal and 'special category data. Back up of servers on premise take place using hardware

encryption via tapes. The WAN link from the school is a dedicated lease line so is not shared with other users like domestic broadband users, therefore it is protected from interception.

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 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). Special education needs, safeguarding information, medical and administration (doctor's 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, bank details, national insurance number, marital status, next of kin, dependents and emergency contacts). Special categories of data (such as gender, age, ethnic group). Contract information (such as start dates, terms and conditions of employment, hours worked, post, roles and salary information, pensions, nationality and entitlement to work in the UK). Work absence information, information about criminal records, details of any disciplinary or grievance procedures. Assessments of performance (such as appraisals, performance reviews, ratings, performance improvement plans and related correspondence). Information about medical or health conditions.

Special Category data? – Some of the personal data collected falls under the UK GDPR special category data. This includes race; ethic origin; religion; biometrics; and health. These may be contained in the Single Central Record, SIMS, child safeguarding files, SEN reports, etc.

How much data is collected and used and how often? – Personal data is collected for all pupils. Additionally, personal data is also held respecting the school's workforce, Board of Governors, Volunteers, and Contractors. Data relating to sports coaches and other

educational specialist is contained within the Single Central Record to ensure health and safety and safeguarding within the school.

How long will you keep the data for? – Consider the data retention period as outlined in the IRMS Information Management Toolkit for Schools and the School's Data Retention Policy.

Scope of data obtained? – 210 pupil (Reception to Year 6). 25 staff members

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)?

The school provides education to its students with staff delivering the National Curriculum

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 and employees to manage the parent/pupil and employment relationship.

Through the Privacy Notice (pupil/workforce) 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? – Access to the files will be controlled by username and password. SIMS is hosting the data and has the ability to access data on instruction of St. Mark's Catholic Primary School who is the data controller for the provision of supporting the service.

The school will be able to upload personal data from its PC for the data to be stored remotely by a service provider. Changes made through the browser when accessing SIMS will update the data stored by the school.

Do they include children or other vulnerable groups? – Some of the data may include special category data such as child safeguarding records, SIMS, SEN records, Single Central

Record. Where the school is using the hosted SIMS solution, the cloud service provider may provide access controls to the files. For example, files designated as private – only you can access the files; public – everyone can view the files without any restriction; and shared – only people you invite can view the files.

Are there prior concerns over this type of processing or security flaws? – Back up of on premise servers take place using hardware encryption via tapes. The WAN link from the school is a dedicated lease line so is not shared with other users like domestic broadband users, therefore it is protected from interception.

St. Mark's Catholic Primary School recognises a number of UK General Data Protection Regulations issues as follows:

- **ISSUE:** Schools using the SIMS hosted cloud based solution will be storing personal data including sensitive information
  RISK: There is a risk of uncontrolled distribution of information to third parties.
  MITIGATING ACTION: All users of SIMS have their own accounts

- **ISSUE**: Transfer of data between the school and the SIMS hosted solution
  RISK: Risk of compromise and unlawful access when personal data is transferred
  MITIGATING ACTION: All data is encrypted at rest and in transit

- **ISSUE:** Understanding the SIMS hosted cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: All data is encrypted at rest and in transit

- **ISSUE:** SIMS hosted 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: SIMS store the majority of Capita ESS customers' personal information in its cloud-based enterprise business systems, which is a combination of Microsoft Dynamics 365, Office365 applications, ServiceNow and Marketo. SIMS

Microsoft Azure datacentres reside in Dublin (Ireland) and all data is encrypted at rest and in transit and complies to ISO27001 standards

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: SIMS Capita is an ICO registered company (registration number Z6674638), fully compliant with UK GDPR data security handling and reporting

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: All personal data will be held in accordance with Capita Plc group policy, and historical records will not be held without a lawful basis

  Capita Plc has a variety of automated retention policies in place that ensure data is regularly cleared down within their system if it has not been used, updated or interacted with in a reasonable amount of time. Essentially Capita Plc will only hold personal information on its systems for the period necessary to fulfill the purposes outlined in its privacy notice.

  Capita Plc recognise that its role remains as data processor and St. Mark's Catholic Primary School is the data controller and therefore will recognise as a default position the data retention periods as outlined in the school' data retention policy

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: SIMS Capita is an ICO registered company (registration number Z6674638), fully compliant with UK GDPR data security handling and reporting

- **ISSUE:** Data is not backed up *(SIMS hosted cloud based solution)*
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: SIMS is ISO 27001 certified which is a recognized accreditation in terms of Information Security Management. ISO 27001 specifies the requirements for

establishing, implementing, maintaining and continually improving an information security management system within the context of Capita SIMS

- **ISSUE:** Data is not backed up *(on premise school based SIMS server)*
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The school recognizes that it is critical that back ups are moved to an alternative media daily, i.e. one that is kept in a physically separate place to the server that is backed up. The school is aware of the need to have a disaster recovery plan (DRP). This includes where they will source a replacement server and what they will do whilst the system is down. The DRP is only worthwhile if on a termly basis, the backups are restored to another machine and proven to work. SIMS data backups stored offsite must be stored in an encrypted format

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Substantial preparation work has been conducted to understand SIMS data flows and client requirements to ensure that they can continue to deliver a service that is compliant post Brexit. SIMS have paid close attention to guidance from the ICO, particularly during the Brexit transition period.

  Many of Capita Plc services are hosted in secure datacentres within the UK and within the EEA. Government guidance states that transfers of personal data from the UK to the EEA can continue unrestricted post-Brexit; however, Capita Plc services are ready to put measures in place should this change, to ensure the continuation of data flows where possible and uninterrupted services for its clients. In circumstances where personal data is being transferred to Capita Plc by their EEA data controller clients for processing in the UK Capita Plc are happy to discuss any measures that may be necessary to adequately protect that data flow.

  Capita Plc continue to monitor guidance from the ICO.

- **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: SIMS has the functionality within the reports menu to handle and respond to Subject Access Requests. The Capita SIMS Privacy Notice recognises the rights of the data subject and provides contact details (dssdataprivacy@capita.co.uk) if a request for a copy for personal information is made

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: St. Mark's Catholic Primary School remains the data controller. SIMS 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: As a service, Capita Plc is UK GDPR compliant. The data processor remains accountable for the data within the system

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

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: SIMS is ISO 27001 certified

- **ISSUE:** The right to be informed; right of access; right of rectification; right to erasure; right to restrict processing; right to data portability; and the right to object
  RISK: The school is unable to exercise the rights of the individual
  MITIGATING ACTION: SIMS provides the technical capability to ensure the school can comply with such requests

  The Capita SIMS Privacy Notice recognises that data subjects have certain rights and if requested, and subject to verification of identity, will exercise such rights within one calendar month

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 processing of this data will allow the school to function safely. We know where our students are at any time and can access the vital information we need to keep them safe. We can build up patterns of academic achievement and attitude so that we can best support our students.

Combined staff and student data allows for timetable creation and school organisation with registers.

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?

As the system is already in use there is no need to consult stakeholders.

Should systems change we would consult more stakeholders.

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 and Workforce). The Legitimate basis includes the following:

- Childcare Act 2006 (Section 40 (2)(a)
- The Education Reform Act 1988
- Further and Higher Education Act 1992,
- Education Act 1994; 1998; 2002; 2005; 2011
- Health and Safety at Work Act
- 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. The cloud based solution 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?

The school will continue to be compliant with its Data Protection Policy

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
Data transfer; data could be compromised	Possible	Severe	Medium
Asset protection and resilience	Possible	Significant	Medium
Data Breaches	Possible	Significant	Medium
Subject Access Request	Probable	Significant	Medium
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 EU, Certified, Penetration Testing and Audit	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
Data Retention	Implementing school data retention periods in the cloud	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Shugufta Hussain / Danielle Linley Sept 22	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	No	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
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:	Shugufta Hussain	The DPO should also review ongoing compliance with DPIA