



Data Protection Impact Assessment (School Life – Covid 19)

Cloud computing is a method for delivering information technology (IT) services in which resources are retrieved from the Internet through web-based tools and applications, as opposed to a direct connection to a server at the school. Bishop Milner Catholic School operates a cloud-based system called School Life. As such Bishop Milner Catholic 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. Bishop Milner Catholic School recognises that moving to a cloud service provider has a number of implications. Bishop Milner Catholic 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 cloud 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. Bishop Milner Catholic 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 DPIA3

Step 2: Describe the processing4

Step 3: Consultation process10

Step 4: Assess necessity and proportionality10

Step 5: Identify and assess risks.....11

Step 6: Identify measures to reduce risk.....12

Step 7: Sign off and record outcomes13



Step 1: Identify 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. The cloud-based system will enable the school to transfer personal data relating to the coronavirus 2 (SARS-Cov-2) which is the virus that causes Covid-19 to Public Health as outlined by the Department of Health/HM Government.

The lawful basis for providing this information is documented in the schools Privacy Notice for Covid Lateral Flow Test/Privacy Notice (Pupil)/Privacy Notice (Workforce)/Privacy Notice (Governors/Volunteers).

Bishop Milner Catholic 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 a cloud-based solution the school aims to achieve the following:

1. Scalability
2. Reliability
3. Resilience
4. Delivery at a potentially lower cost
5. Supports mobile access to data securely
6. Good working practice

The cloud service provider cannot do anything with the school's data unless they have been instructed by the school. The schools Privacy Notice will be updated especially with reference to the storing of pupil in the cloud.



Step 2: Describe the processing

The Privacy Notices (pupil) for the school provides the legitimate basis of why the school collects data. The lawful basis in order to process personal data in line with the 'lawfulness, fairness and transparency principle is as follows:

This information is processed and shared under obligations set out in Public Health legislation under Regulations 3(1) and (4) of the Health Service (Control of Patient Information) Regulations 2002 (COPI) which allows the sharing of data for COVID related purposes.

The school has highlighted Article 6(1)(e) 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller as their lawful basis.

It would also be lawful to disclose any requested information as a consequence of an exemption that exists within the Data Protection Act 2018. Schedule 2, Part 2 paragraph 7 – where processing is required for functions designed to protect the public. In this case sub paragraph 4 is likely to apply:

4. The function is designed to

- a. To secure the health, safety and welfare of persons at work, or
- b. To protect persons other than those at work against risk to health or safety arising out of or in connection with the action of persons at work

This exemption applies where the function is of a public nature and is exercised in the public interest.

In all disclosure cases, the school will satisfy itself that the request has originated from an authenticated source, i.e. Public Health who is working on behalf of the NHS England.

The school will only provide information that is necessary for the activity. Any special category data needs to be communicated via secure means.

This is recorded in Bishop Milner Catholic School Privacy Notice for Covid Lateral Flow Test/Privacy Notice (Pupil)/Privacy Notice (Workforce)/Privacy Notice (Governors/Volunteers).

How will you collect, use, store and delete data? – The information collected relates to a positive or negative PCR Test, the date of the PCR test, date of isolation (where applicable), earliest date of return and likely source of infection. School Life also collects information about close contacts



including the name, address, e-mail and mobile phone numbers of family members, social groups, and close contacts.

The information is retained according to the school's Data Retention Policy.

What is the source of the data? – The information is obtained from the data subject and completed online via School Life.

Will you be sharing data with anyone? – Bishop Milner Catholic School will share information with the Local Authority (Public Health), NHS Health Services, and the Department for Education.

What types of processing identified as likely high risk are involved? – Transferring personal data from the school to the cloud. Storage of personal data in the Cloud.

What is the nature of the data? – The information collected relates to a positive or negative PCR Test, the date of the PCR test, date of isolation (where applicable), earliest date of return and likely source of infection. School Life also collects information about close contacts including the name, address, e-mail and mobile phone numbers of family members, social groups, and close contacts.

Special Category data? – The personal data falls under the UK GDPR special category data. This includes health details.

How much data is collected and used and how often? – Personal data is collected for all pupils, workforce, and volunteers based on positive or negative PCR tests.

How long will you keep the data for? – The school will consider the data retention period as outlined by Public Health and the NHS.

Scope of data obtained? – 874 pupils.

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

What is the nature of your relationship with the individuals? – Bishop Milner Catholic School collects and processes personal data relating to its pupils and employees to manage the parent/pupil and employment relationship.

Through the Privacy Notice for Covid Lateral Flow Test/Privacy Notice (Pupil)/Privacy Notice (Workforce)/Privacy Notice (Governors/Volunteers) Bishop Milner Catholic 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? – School Life will provide a log in for the school. The school can then report the results of a PCR test through School Life. Passwords are not stored, a hashed representation of the password is created and associate with the account.

Do they include children or other vulnerable groups? – The personal data falls under the UK GDPR special category data. This includes health details.

Are there prior concerns over this type of processing or security flaws? – All data kept on School Life servers are encrypted. Log in to the School Life portal is via a strong SHA-2/2048-bit encryption. School Life uses Amazon Web Services which is certificated to certain security and regulations including ISO 27001 and PCI Data Security Standard.

In terms of application security, users (parents, pupils, staff) can log into the School Life IOS and android mobile applications and view user specific data. School Life have a number of options to control the level of access to data for a user.

Bishop Milner Catholic School has the responsibility to consider the level and type of access each user will have.

Bishop Milner Catholic School recognises that moving to a cloud-based solution raises a number of UK General Data Protection Regulations issues as follows:

- **ISSUE:** The 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: The School Life administration system can only be accessed via authenticated users that have been granted the role of staff members. Only existing staff members or School Life administrators can grant this level of authorization. User passwords are not stored in the system – one-way cryptographic hash is created in their place
- **ISSUE:** Transfer of data between the school and the cloud
RISK: Risk of compromise and unlawful access when personal data is transferred
MITIGATING ACTION: Access at server level is restricted to senior members of staff and are only accessible across a secure VPN who ensure that the lasts patches updates are installed. All data kept on



the School Life database servers are encrypted, whilst login to the School Life portal is via strong SHA-2/2048-bit encryption

- **ISSUE:** Understanding the cloud-based solution chosen where data processing/storage premises are shared?
RISK: The potential of information leakage
MITIGATING ACTION: Amazon EC2 cloud infrastructure is certified to certain security and regulations including ISO 27001 and the PCI Data Security Standard. All School Life servers are located behind firewalls and only ports and services that are deemed necessary are opened

- **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: School Life uses Amazon EC2 to host School Life servers, which in turn hosts the personal data which is uploaded from the school. School Life would keep the school's data on its systems for as long as a relationship exists between the school and School Life

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
RISK: UK GDPR non-compliance
MITIGATING ACTION: School Life's Privacy Notice states that the school has a right to access any personal information that School Life processes including what personal data is held, the purposes of the processing, categories of personal data concerned, recipients to whom the personal data has/will be disclosed, how long School Life stores the information, and information about the personal data source. If School Life receives a request from the school to exercise any of these rights, School Life may ask the school to verify its identity before acting on the request; this is to ensure that the data is protected and kept secure

As part of its commitment to privacy and security, when a school contacts the support desk, schools will be asked to confirm specific details to confirm that it is a genuine call/request. School Life will always assist schools, where possible, in meeting their obligations under UK GDPR

- **ISSUE:** Implementing data retention effectively in the cloud
RISK: UK GDPR non-compliance
MITIGATING ACTION: The personal data will be managed in line with the school's data retention policy. School Life only ever retains personal information for as long as is necessary. School Life actively reviews its Privacy Policy to meet these obligations. School Life will keep school data on its systems for as long as a relationship exists between the school and School Life. Additionally,



every entry on the 'School Life' platform will be fully cleansed of content and data within 30 days of the contract with the particular school ending

- **ISSUE:** Data Back ups

RISK: UK GDPR non-compliance

MITIGATING ACTION: School Life use Amazon Web Services (AWS) back up services. AWS back up is a fully managed, policy-based backup solution that makes it easy to automatically back up the School Life application data across AWS services in the cloud

AWS back up's policies provide automated backup scheduling, back up retention management, and lifecycle rules, which assists in streamlining back up processes. AWS backup supports backing up EBS volumes, RDS databases, DynamoDB tables, EFS file systems, and Storage Gateway volumes and stores School Life back up data durably and securely using Amazon S3. AWS back up's centralised back up monitoring, back up encryption, and back up access policy features help School Life to meet internal and regulatory backup compliance requirements

- **ISSUE:** Responding to a data breach

RISK: UK GDPR non-compliance

MITIGATING ACTION: The system has passwords for every School Life staff member. Data breaches can be dealt with by any member of staff as a result. Every member of School Life staff is trained in how to shut down the system if required whilst any data breach is dealt with. Every member of staff has signed a confidentiality agreement. Passwords are changed every three months automatically and are alpha numerical. They are not recorded on any file. All accesses to the system from School Life staff or school side are logged and stamped with date and time. All School Life staff are trained in how to deal with data breaches and a written policy and procedure exists

- **ISSUE:** Post Brexit

RISK: UK GDPR non-compliance

MITIGATING ACTION: School Life use Amazon S3 to host its database and related programs. The data is currently stored on servers in Eire. Servers are also based on the UK mainland and can be switched post Brexit.

- **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: School Life have a written data Subject Access Request policy and procedure. School Life staff are trained in what to do when a request comes in. SARs are managed the UK GDPR data manager, or in their absence, by two deputies on behalf of the school



- **ISSUE:** Data Ownership
RISK: UK GDPR non-compliance
MITIGATING ACTION: School Life does not share or disclose any of the school's personal information without the school's consent. School Life uses third parties to provide the service, e.g. Amazon EC2 for storing data in the cloud. However, all processors acting on the behalf of School Life only process school data in accordance with instructions from School Life and in compliance with School Life's Privacy Notice, data protection law, and any other appropriate confidentiality and security measures

- **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: This should be monitored to address any changes in technology and its impact on data to 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 School Life

- **ISSUE:** Security of Privacy
RISK: UK GDPR non-compliance
MITIGATING ACTION: Personal information used in the 'School Life' platform is always kept to a minimum and is only visible by staff elected by the school. School Life will not access this information unless it is deemed necessary to do so for the purposes of support and in any instance will only access this information with permission from the school

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

1. Scalability
2. Reliability
3. Resilience
4. Delivery at a potentially lower cost
5. Supports mobile access to data securely
6. Good working practice



Step 3: Consultation process

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

The lawful basis for processing personal data is contained in the school's Privacy Notice for Covid Lateral Flow Test/Privacy Notice (Pupil)/Privacy Notice (Workforce)/Privacy Notice (Governors/Volunteers). The lawful basis includes the following:

Public Health legislation under Regulations 3(1) and (4) of the Health Service (Control of Patient Information) Regulations 2002 (COPI) which allows the sharing of data for COVID related purposes.

Article 6(1)(e) 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller as their lawful basis.

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
Data Transfer	Secure network, end to end encryption	Eliminated reduced accepted	Low medium high	Yes/no
Asset protection & resilience	Data Centre in EU. Accredited to ISO 27001 and PCI Data Security Standard	Reduced	Medium	Yes
Data Breaches	School Life's ability to respond and deal with a data breach	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
				Yes



Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Siobhan Foster	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Siobhan Foster	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: (1) Functionality of School Life to respond to a data breach (2) Technical capability to ensure the school can comply with a data subject access requests (3) School to take into consideration backups and if the data is stored in multiple locations and the ability to remove the data in its entirety (4) Contingency arrangements around a no deal Brexit		
DPO advice accepted or overruled by: [YES/NO] If overruled, you must explain your reasons		
Comments: YourIGDPO Service liaised with supplier for further clarification as outlined above in summary of DPO advice.		
Consultation responses reviewed by: If your decision departs from individuals' views, you must explain your reasons		
Comments: [Comments provided]		
This DPIA will kept under review by:	Gabriela Roden	The DPO should also review ongoing compliance with DPIA