Data Protection Impact Assessment

(Information Society Services/third party apps)

The ICO define Information Society Services as "any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service."

Similarly, a third party app is an application created by a developer that isn't the manufacturer of the device the app runs on or the owner of the website that offers it. Third party apps commonly used by schools will access pupil profile information from, for example, the school's Management Information System. Dependent on the type of information accessed this may include special category data such as education health care plans, and safeguarding information.

Section 3 Article 35 (1) states "Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."

Bishop Milner Catholic College uses third party and/or Information Society Services apps. As such Bishop Milner Catholic College must consider the privacy implications of such apps. 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 College recognises that using a third party and/or Information Society Services apps provider has a number of implications. Bishop Milner Catholic College 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 a third party and/or Information Society Services apps 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. If stored in the cloud, 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 taken are sufficient, and that the rights of the data subject under the UK GDPR is satisfied by the school.

Bishop Milner Catholic College recognizes that changes do occur and on this basis good practice recommends that the school review its Data Protection Impact Assessment.

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

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? – The use of the third party and/or Information Society Services app will enhance the educational experience, deliver a cost effective solution, and help meet the needs of the business.

Bishop Milner Catholic College 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 third party and/or Information Society Services app the school aims to achieve the following:

1. Scaleability
2. Reliability
3. Management
4. Delivery at a potentially lower cost
5. Supports mobile access to data securely
6. Update of documents in real time (where applicable)
7. Good working practice, i.e. security of access

[School to insert any other reasons as appropriate]

There are numerous third party apps used by schools. They provide learning platforms which can be pupil specific, providing lesson plans for marking and tracking progress. They can also identify learning needs of pupils, using adaptive learning for students to learn at their own pace. Some apps may provide information for parents on their child's educational strengths and weaknesses.

Information Society Services apps are invariably web based and use personal data to set up individual log ins.

The third party app and/or Information Society 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 third party and/or Information Society Service.

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. 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.

Will you be sharing data with anyone? – Bishop Milner Catholic College 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, Management Information Systems and various third party Information Society Services applications.

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

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). This may also include date of birth, country of birth, free school meal eligibility. Other information collected may include attendance, assessment, and attainment information. The school may also obtain data on parents/guardians/carers including their name, address, telephone number and e-mail address.

Special Category data? – Some of the personal data collected falls under the UK GDPR special category data. This includes race; ethic origin; religion; Children Looked After, Special Education Needs, biometrics; and health. These may be contained in the Single Central Record, and the school's management information system.

How much data is collected and used and how often? – Personal data is collected for all pupils.

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

Scope of data obtained? – pupils, workforce, governors, volunteers

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 College collects and processes personal data relating to its pupils and parents to manage the parent/pupil relationship.

Through the Privacy Notice (Pupil) Bishop Milner Catholic College 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. If cloud based the provider hosting the data will not be accessing it without the expression permission of [insert Name of School].

The school will be able to upload personal data from its PC for the data to be stored remotely by a service provider. 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? – Personal data will relate to pupils attending the school. If located in the school appropriate password permissions would be insitu. If a cloud service provider then access controls would be put in place.

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

- ISSUE: Information Society Service will be storing personal data including sensitive information
  RISK: There is a risk of uncontrolled distribution of information to third parties. MITIGATING ACTION: Consider the use of an authentication process, for example, using a username and password system, cloud users must each have their own accounts

- ISSUE: Lawful basis for processing personal data
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: School has included the Information Society Service apps in its Privacy Notice (Pupil), (Workforce), and (Governors and Volunteers) which identifies the lawful basis for processing personal data

- ISSUE: Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The school maintains ownership of the data. In terms of disclosure third party apps will not release the information to any third party unless the request is subject to legal obligation without obtaining the express written authority of the school who provided the information

- ISSUE: Data Retention
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: 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

- 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: Third party processor and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: The school is unable to exercise the rights of the individual
  MITIGATING ACTION: Information Society Services app will need to provide the technical capability to ensure the school can comply with such requests. This may be included as part of the contract

- ISSUE: Post Brexit
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: What does the third party processor intend to do to allow data processing in the UK to remain compliant

- 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: Providers will need to provide the technical capability to ensure the school can comply with a data subject access requests. This may be included as part of the contract

- ISSUE: Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The school must assess what kind of security and privacy measures are in place. Cloud providers can demonstrate compliance through a DPIA, being ISO 27001 certified, etc

  If cloud based the following applies

- ISSUE: Transfer of data between the school and the cloud
  RISK: Risk of compromise and unlawful access when personal data is transferred. MITIGATING ACTION: Encryption ensures data 'in transit' between endpoints should be secure and protected from interception. This can be achieved by using an encrypted protocol or other secure methods

- 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. The school should maintain ownership of the Cloud technologies used ensuring current and future technologies enable UK GDPR compliance

- 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: To determine the privacy rules which apply based on the location of the cloud

- ISSUE: Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: It is advisable that the school tailor any contract to incorporate these privacy commitments

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

- Scaleability
- Reliability
- Resilience
- Delivery at a potentially lower cost
- Supports mobile access to data securely
- Update of documents in real time
- Good working practice, i.e. secure access to sensitive files

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 (Pupil). 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)

[School to insert any other legitimate basis as appropriate]

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
Post Brexit (GDPR noncompliance)	Possible	Significant	Medium
Subject Access Request	Probable	Significant	Medium
Data Retention	Probable	Significant	Medium
[School to insert other information as appropriate]			

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	
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
Post Brexit	Contingency plans in place	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
	[School to insert other information as appropriate]			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)* Does [insert name of app] 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?)* *(2)* Does the functionality exist to enable the school to respond to subject access requests? *(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)* (4) What certification does [insert name of app] have?, *(e.g. ISO 27001 certified, etc)*		
DPO advice accepted or overruled by: [Yes/No] If overruled, you must explain your reasons		
Comments: [DPO Advice provided]		
Consultation responses reviewed by:[Insert name] 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