Data Protection Impact Assessment (Sharepoint)

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. Thorns Primary School operates a cloud based system. As such Thorns 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.

Thorns Primary School recognises that moving to a cloud service provider has a number of implications. Thorns 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 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. Thorns 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

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? – Thorns Primary School To move electronic storage from a local server to a cloud based solution. This will deliver a cost effective solution, rationalizing storage of data, to meet the needs of the business. It will assist agile working enabling staff to work remotely and ensure information security (removing the need for memory sticks, etc).

Thorns 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 a cloud based solution the school aims to achieve the following:

1. Scaleability
2. Reliability
3. Resilience
4. Delivery at a potentially lower cost
5. Supports mobile access to data securely
6. Update of documents in real time
7. Good working practice, i.e. secure access to sensitive files

The school currently has its personal data stored locally via dedicated servers held on site. Personal data is accessible via servers to desk top computers. The information is held securely with personal data backed up from the drive every 24 hours. The network is only accessible through dedicated password linked to individual members of staff.

The benefits of moving to the cloud means that information can be grouped appropriately, Thorns Primary School knows where all personal data is held and can set permissions accordingly. Cloud based systems enable the school to upload documents, photos, videos, and other files to a website to share with others or to act as a backup copy. These files can then be accessed from any location or any type of device (laptop, mobile phone, tablet, etc).

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 and workforce data in the cloud.

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. The cloud will provide a more structured environment with appropriate permission levels set to view data.

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. For more information please consult Thorns Primary School Privacy Notices.

Will you be sharing data with anyone? – Thorns 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, RM Integris and various third party Information Society Services applications.

Thorns 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 the cloud. Storage of personal and 'special category 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). 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 (doctors 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, RM Integris, 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

Scope of data obtained? – How many individuals are affected (pupils, workforce, governors, volunteers)? And what is the geographical area covered? Year 1 to Year 6 pupils [189], workforce [33], Board of Governors [9], and Volunteers, and any other, i.e. contractors, education specialists.

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? – Thorns 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) Thorns 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. Cloud Service provider is hosting the data and will not be accessing it.

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? – Some of the data may include special category data such as child safeguarding records, RM Integris, SEN records, Single Central Record. 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? – Does the cloud provider store the information in an encrypted format? What is the method of file transfer? For example, the most secure way to transfer is to encrypt the data before it leaves the computer. Encryption does have its limitations inasmuch as the encryption key will need to be shared with others to access the data.

Thorns Primary 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:** Sharepoint sits within Office Microsoft 365. Office Microsoft 365 sits within Microsoft Azure which provides a secure cloud based service
- **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 is identified in the UK GDPR as a protective measure that renders personal data unintelligible when it is affected by a breach
  Microsoft products and services such as Azure, Dynamics 365, Enterprise Mobility + Security, Office Microsoft 365, SQL Server/Azure SQL Database, and Windows 10 offer robust encryption for data in transit and data at rest

- **ISSUE:** Use of third party sub processors?
  RISK: Non compliance with the requirements under UK GDPR
  MITIGATING ACTION: Microsoft shares data with third parties acting as its sub processors to support functions such as customer and technical support, service maintenance, and other operations

- Any subcontractors to which Microsoft transfers Customer Data, Support Data, or Personal Data will have entered into written agreements with Microsoft that are no less protective than the Data Protection Terms of the Online Services Terms. **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage.
  MITIGATING ACTION: Microsoft products and services such as Azure, Dynamics 365, Enterprise Mobility + Security, Office Microsoft 365, SQL Server/Azure SQL Database, and Windows 10 offer robust encryption for data in transit and data at rest

- **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: Please note that Microsoft don't tell you which country or offer an option to pick a specific country (e.g. UK)

  However, Microsoft do have a level of granularity for some parts of Office 365 (Exchange Online, SharePoint, etc) as follows:

  (1) Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments);
  (2) SharePoint Online site content and the files stored within that site;
  (3) files uploaded to OneDrive for Business, and;
  (4) project content uploaded to Project Online

Nevertheless, in any event, Microsoft will ensure that transfers of personal data to a third country or an international organization are subject to appropriate safeguards as described in Article 46 of the UK GDPR

In addition to Microsoft commitments under the Standard Contractual Clauses for processors and other model contracts, Microsoft is certified to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks and the commitments they entail

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: When operating as a processor, Microsoft makes available to schools, as data controllers, the personal data of its data subjects and the ability to fulfill data subject access requests when they exercise their rights under the UK GDPR. This is done in a manner consistent with the functionality of the product and Microsoft's role as a processor

  If Microsoft receive a request from the school's data subjects to exercise one or more of their rights under the UK GDPR, Microsoft redirect the data subject to make its request directly to the data controller, i.e. the school. The Office 365 Data Subject Requests Guide provides a description to the data controller on how to support data subject rights using the capabilities in Office 365

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: As set out in the Data Protection Terms in the Online Services Terms, Microsoft will retain Customer Data for the duration of the school's right to use the service and until all the school's data is deleted or returned in accordance with the school's instructions or the terms of the Online Services Terms

  At all times the school will have the ability to access, extract, and delete personal data

stored in the service, subject in some cases to specific product functionality intended to mitigate the risk of inadvertent deletion

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Microsoft products and services—such as Azure, Dynamics 365, Enterprise Mobility + Security, Microsoft Office 365, and Windows 10—have solutions available today to help a school detect and assess security threats and breaches and meet the UK GDPR's breach notification obligations

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Microsoft currently only promise to store Microsoft Teams data within the EU. Please note that they don't tell you which country or offer an option to pick a specific country (e.g. UK)

  Nevertheless, in any event, Microsoft will ensure that transfers of personal data to a third country or an international organization are subject to appropriate safeguards as described in Article 46 of the UK GDPR

  In addition to Microsoft commitments under the Standard Contractual Clauses for processors and other model contracts, Microsoft is certified to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks and the commitments they entail

- **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: Microsoft provides the ability to access, export, and delete system-generated logs that may be necessary to complete a Data Subject Access Request. Examples of such data may include: (1) product and service usage data such as user activity logs; (2) user search requests and query data; and (3) data generated by product and services resulting from system functionality and interaction by users or other systems

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance

MITIGATING ACTION: Microsoft is the data processor, processing the school's personal data through the use of Sharepoint. The school as data controller still has ownership of the data

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Microsoft is committed to helping protect the security of the school's information. In compliance with the provisions of Article 32 of the UK GDPR, Microsoft has implemented and will maintain and follow appropriate technical and organizational measures intended to protect Customer Data and Support Data against accidental, unauthorized, or unlawful access, disclosure, alteration, loss, or destruction

  Microsoft is subject to independent verification of its security, privacy, and compliance controls. In order to provide this, Microsoft undergo several independent third-party audits on a regular basis. For each one, an independent auditor examines Microsoft's data centres, infrastructure, and operations.

  The following are examples of Microsoft's accreditation:

ISO 27001: is one of the most widely recognized, internationally accepted independent security standards. Microsoft has earned ISO 27001 certification for the systems, applications, people, technology, processes, and data centres that make up its shared Common Infrastructure

ISO 27017: is an international standard of practice for information security controls based on ISO/IEC 27002, specifically for Cloud Services. Microsoft has been certified compliant with ISO 27017 for its shared Common Infrastructure

ISO 27018: is an international standard of practice for protection of personally identifiable information (PII) in Public Cloud Services. Microsoft has been certified compliant with ISO 27018 for its shared Common Infrastructure

The American Institute of Certified Public Accountants (AICPA) SOC 2 (Service Organization Controls) and SOC 3 audit framework defines Trust Principles and criteria for security, availability, processing integrity, and confidentiality. Microsoft has SOC 1, SOC 2 and SOC 3 reports for its shared Common Infrastructure

This means that independent auditors have examined the controls protecting the data in Microsoft's systems (including logical security, privacy, and data centre security), and assured that these controls are in place and operating effectively

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:

- 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

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 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
Post Brexit (GDPR noncompliance)	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
Post Brexit	Contingency plans in place	Reduced	Significant	Medium
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

15

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Rebecca Jordan	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Rebecca Jordan	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)* 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 the information stored?)* (4) What is the method of file transfer from school to the remote server and vice versa? *(is it via a secure network?)* (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 the cloud provider have?, *(e.g. ISO 27001 certified, etc)*		
DPO advice accepted or overruled by: No If overruled, you must explain your reasons		
Comments: DPO Advice provided		
Consultation responses reviewed by: N/A If your decision departs from individuals' views, you must explain your reasons		
Comments: Comments provided		
This DPIA will kept under review by:	Karen Cartwright	The DPO should also review ongoing compliance with DPIA