Data Protection Impact Assessment (SchoolMoney)

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 several 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 considering 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? – SchoolMoney is a secure online payments system enabling parents to pay for school dinners (enabling the school to pre book school meals), breakfast and after school club(s), uniform and school trips (giving consent and allowing payment). Parents can make online banking payments or make school payments in supermarkets, newsagents and post offices. Parents create an online account by providing primary contact details linked to their child. There is also the additional functionality of SchoolMoney app by which the school can communicate with the parent. SchoolMoney helps to deliver a cashless and cost effective solution to the school.

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. Scalability
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. moving to a cashless environment

SchoolMoney (Eduspot Ltd) is a cloud based system which enables the school to collect payments online for school services such as catering. SchoolMoney can be accessed from any location or any type of device (laptop, mobile phone, tablet, etc) via SchoolMoney app.

BehaviourWatch, ParentsEvening, Teachers2Parents, School Pod and SchoolsWire are Eduspot services supporting schools.

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 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) for the school provides the lawful basis of why the school collects personal data.

How will you collect, use, store and delete data? – Limited information about pupils, staff and parents is retrieved through the school's management information system and/or uploaded by the school. Additional information relating to parent/guardian may be added by the school to support family circumstances where appropriate. The information is retained according to the school's Data Retention Policy.

What is the source of the data? – Information about pupils is drawn from the school's management information system.

SchoolMoney provides a secure Parent Account accessed via the Parent Login or App, which, upon provisioning login details allows parents to access information provided by their child's school and to make Parent Payments to Thorns Primary School. By providing the login details parents agree for SchoolMoney to communicate with them via e-mail and/or SMS and/or via the Parent Login and/or App notifications.

During the provisioning of the Parent Account the parent will be provided with a unique encrypted password. The parent may change this password once the parent has gained access to the Parent Login. A parent may be requested to change their password from time to time.

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, SchoolMoney and various third party Information Society Services applications.

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? – SchoolMoney collects the following information:

Pupil – SchoolMoney service imports the following data fields. Management information system ID, Admissions Number, Name, Gender, and Registration and Year Group. The following is optional: Free School Meal status, Admissions Status, Meal Information (Dinner Money), Dietary Needs, Medical Conditions.

Workforce – Management information system ID, Name.

Parental Responsibility of one or more pupils (Priority 1 contacts) – Management information system ID, Name, E-mail, Mobile phone number, Parental Responsibility and Priority.

Credit card/debit card information is handled by SchoolMoney's payment provider (Secure Trading). Secure Trading does not have access to the SchoolMoney platform and is only used in the process of making payment by the parent.

Special Category data? – Some of the personal data collected falls under the UK GDPR

special category data. This includes information relating to health and religion. The lawful basis for collecting this information relates to Article 9 2 (g) *processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.*

How much data is collected and used and how often? – Personal data is collected for all pupils. The collected information includes names, e-mail addresses and phone numbers. Contact details which may include e-mail and mobile number is also collected from parents. Where data is collected automatically from the management information system this is undertaken nightly and manual imports can be undertaken by the school at any time.

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, and volunteers)? And what is the geographical area covered? Reception, Year 1 to Year 6 pupils 195, parents/carers 195.

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 to manage the parent/pupil and school relationship. This includes managing, and the provision of, school catering, school trips and providing a wrap around care facility.

Through the Privacy Notice (Pupil) 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. SchoolMoney (Eduspot Ltd) is hosting the data and has the ability to access data on instruction of Thorns 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 management information system for the data to be stored remotely by a service provider. This will be achieved through a data sharing facility called Wonde. Management information system synchronization can be manually triggered at any time by running SchoolMoney's MIS sync tool. Any uploaded/manually entered records can be updated at any time via the SchoolMoney website. Changes made to SchoolMoney are not written back to the school's MIS and therefore any data corrections should be made in the MIS for the benefit of all connected systems used by the school. SchoolMoney does not allow editing of records that are source from the school's MIS.

Do they include children or other vulnerable groups? – SchoolMoney contains personal data relating to children. However, SchoolMoney will not differentiate between those children that have safeguarding records or SEN records, etc. The cloud service provider may provide access controls to 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? – All data is encrypted in SchoolMoney. Data transfer is secured by TLS 1.2.

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: SchoolMoney implements suitable input control measures including authentication of the authorized personnel; protective measures for the data input into memory, utilisation of unique authentication credentials or codes

(passwords), and automatic log off of user ID's that have not been used for a substantial period of time. All users of SchoolMoney have their own accounts

- **ISSUE**: Transfer of data between the school and the cloud
  RISK: Risk of compromise and unlawful access when personal data is transferred.
  MITIGATING ACTION: SchoolMoney implements suitable measures to prevent the personal data from being read, copied, altered or deleted by unauthorized parties during transmission. The various measures include use of adequate firewall, VPN and encryption technologies. Special category data and highly confidential personal data such as National ID numbers, credit or debit card numbers are also encrypted in the system. SchoolMoney also provides user alerts upon the incomplete transfer of data (end to end check); and as far as possible, all data transmissions are logged, monitored and tracked

- **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: All data is AES encrypted at rest (Bitlocker) and in transit (TLS 1.2). The platform operates from our dedicated datacentre in Leicester, subject to SchoolMoney's physical security controls, personnel access policies, and diverse routing of communications and power. SchoolMoney's Cashless Catering integration service and platform backups are operated from Microsoft Azure Dublin and subject to Microsoft's stringent multi-tenant controls

- **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: All service elements are located within the EEA and subject to UK GDPR. The servers hosting SchoolMoney are located in Leicester, UK. The platform backups and the Cashless Catering integration service are located in Microsoft Azure Dublin, Ireland

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: SchoolMoney will promptly notify the school as data controller if it receives a request from a data subject to access, rectify or erase that individual's personal data, or if a data subject objects to the processing of, or makes a data portability request. SchoolMoney will not respond to the request without the data controllers consent. SchoolMoney will provide reasonable assistance to facilitate such requests

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
- **MITIGATING ACTION:** SchoolMoney is fully compliant with UK GDPR data security retention and storage. SchoolMoney has data deletion functionality

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: SchoolMoney as soon as reasonably practicable upon becoming aware of any breach of security will notify the school as data controller

- **ISSUE:** Engaging third-party sub processors
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Eduspot Ltd maintains an up to date list of its sub processors. If the school has a reasonable objection to any new or replacement sub processor, it can notify Eduspot Ltd in writing within 10 days of the notification and both parties will seek to resolve the issue. Eduspot Ltd when engaging any sub processor will do so on the basis of a written contract which will require them to meet the same terms and conditions as set out in the Data Protection Addendum in order for the third party to meet its data protection obligations

- **ISSUE:** Transfer of personal data outside the EEA
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: All data is stored within the EEA. If Eduspot Ltd transfers any personal data to a sub processor located outside of the EEA it will ensure, in advance of any such transfer, ensure that the legal mechanism to achieve adequacy of that

processing is in place. This will include, where applicable, standard contractual clauses approved by EU authorities under EU Data Protection Laws, certified under the EU-US Privacy Shield Framework; and/or the existence of any other specifically approved safeguard for data transfers as recognised under EU Data Protection Laws

The European Court of Justice (ECJ) has ruled that the EU-US Privacy Shield is invalid as it fails to protect privacy and data protection rules. As part of the same ruling the ECJ decided that another data transfer mechanism, Standards Contractual Clauses, or SCCs, remain valid. The school will need to confirm whether an SCC is in place

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Eduspot Ltd current and Post Brexit statement can be found here (Brexit Business Continuity Statement)

- **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: SchoolMoney will promptly notify the school as data controller if it receives a Subject Access Request. SchoolMoney will not respond to the request without the data controllers consent. SchoolMoney will provide reasonable assistance to facilitate such Subject Access Requests

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The school remains the data controller. SchoolMoney (Eduspot Ltd) 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: SchoolMoney implements suitable measures to ensure that data collected for different purposes can be processed separately including the application of appropriate security measures for the appropriate users; modules within SchoolMoney

separate which data is used for which purposes, i.e. by functionality and function. At the database level, data is stored in different normalised tables, and separated per module, per data controller or function they support. Interfaces, batch processes and reports are designed for only specific purposes and functions, so data collected for specific purposes is processed separately

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

- **ISSUE:** Back up of data
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Back up of data is stored in an alternative site and is available for restore in case of failure of the primary system

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: SchoolMoney ensures that it implements suitable measures to prevent its data processing systems from being used by unauthorized persons and access controls for use in specific areas of its data processing systems. These include the use of encryption technologies, automatic temporary lock out of users, monitoring of break in attempts, limited access rights to personal data, etc

  Microsoft Azure Dublin (where SchoolMoney Cashless Catering integration service and platform backups are located) is certified ISO 27001

  ICO registration number is Z9637161, the data controller is named as Teachers2Parents Ltd (which is part of the portfolio of services offered by Eduspot Ltd)

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:

- Scalability
- 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. moving to a cashless environment

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. Parents will be made aware of the benefits of a cashless and cost effective solution. 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 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 wwddew
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:	**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)* What is the source of the data? *(2)* Where is the server located? (3) What is the method of file transfer from school to the remote server and vice versa? (4) What certification does the cloud provider have? (5) Is the provider ICO registered?		
DPO advice accepted or overruled by: **No** If overruled, you must explain your reasons		
Comments:		
Consultation responses reviewed by: **N/A** If your decision departs from individuals' views, you must explain your reasons		
Comments:		
This DPIA will kept under review by:	**Karen Cartwright**	The DPO should also review ongoing compliance with DPIA