Straits primary School

Data Protection Impact Assessment (ParentHub)

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. Straits Primary School operates a cloud based system called ParentHub. As such Straits 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.

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

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 contact those with parental responsibility in a timely and efficient way.

ParentHub is first and foremost a communication platform, helping schools share and retrieve information. ParentHub can be accessed by the user via mobile devices.

There is an expectation that parents will be updated in a timely manner about anything that will impact upon their child whilst they are at the school. The most appropriate method to provide parents with this information is via ParentHub which will ensure that important messages are delivered to parents without reliance on the pupil.

The school may, for example, post details of school closure on its website or via a local radio station. However, there is no guarantee that this information may reach those with parental responsibility in a timely manner.

The text messaging service will only be used to inform parents of school activities and issues which may impact on the child. Consent has been identified as the lawful basis for processing personal data in the Straits Primary School Privacy Notice (Pupil).

The school will be complying with Safeguarding Vulnerable Groups Act, and Working together to Safeguard Children Guidelines (DfE). Straits 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. Good working practice

The school currently uses Parent Hub to provide information regarding a child's attendance, health and safety notices, school closure, school trip information, etc. It will continue to use contact information obtained from the data subject which is stored in the school's management information system

ParentHub will enable the user to access information 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 in the cloud.

Step 2: Describe the processing

Describe the nature of 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:

6.1 (c) Processing is necessary for compliance with a legal obligation to which the controller is subject; e.g. health & safety and safeguarding
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
6.1 (f) Processing is necessary for the purposes of the legitimate interest pursued by the controller or by a third party

The school has highlighted consent as the lawful basis by which it processes personal data. This is recorded in Straits Primary School Privacy Notice (Pupil). The school needs to determine what lawful basis it intends to use. If there is real choice then consent is appropriate and if there is no choice then a legitimate interest assessment would be appropriate.

How will you collect, use, store and delete data? – The information collected by the school is retained on the school's management information system. ParentHub also collects information from online contact forms, import of data from the school management information system, verbal and written from nominated administrator contact within the school. 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.

Will you be sharing data with anyone? – Straits 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.

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

Describe the scope of the processing: Pupil data relates to personal identifiers and contacts (such as name and their school groups – classes, years, etc).

The Privacy Policy for ParentHub states that the following personal data will be collected: The names of students and their school groups (classes, years etc.); the names of any parents, guardians, carers or other student contacts along with their mobile phone numbers and email addresses; and the names of staff members and their mobile phone numbers.

The school will ensure that it has the authority to share data with ParentHub on behalf of the school; it has obtained the lawful basis to provide the personal information of any individual to ParentHub and have obtained all necessary consent to contact any individual through the Services (via the ParentHub application, or by email or SMS).

It also states under the 'data minimization' principle that ParentHub will never collect any unnecessary personal data from the school and will not process school information in any way, other than that specified in the Privacy Notice for ParentHub.

The information is sourced from Straits Primary School from the management information system either via manual import or automated transfer.

Special Category data? – None 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 and their respective parent/guardians. Additionally personal data is also held respecting school administrative contact details, school name and address, school e-mail address, school contact telephone number, and staff information (staff name, staff e-mail address, staff teaching groups).

How long will you keep the data for? – in line with 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? Reception and Year 1 to Year 6 pupils 406 and workforce 60.

Describe the context of the processing:

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

What is the nature of your relationship with the individuals? – Straits 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) Straits 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? – ParentHub users (students, parents, staff) may have individual user accounts to log into ParentHub to retrieve communications. 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? – None of the data is classified under UK GDPR as special category. However, personal data will be collected: pupil information including the pupil name, pupil UPN (unique pupil number), and pupil class name.

Are there prior concerns over this type of processing or security flaws? – All data kept on ParentHub servers are encrypted at rest using 256-bit Advanced Encryption Standard (AES) encryption. ParentHub secure identity server encrypts user access credentials that are required to access ParentHub. ParentHub stores its data within Microsoft's Azure cloud infrastructure which is managed in compliance with multiple regulations, standards and best-practices, including ISO/IEC 27001, ISO/IEC 27018, SOC 1, SOC 2 and UK G-Cloud

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

Straits Primary School has the responsibility to consider the level and type of access each user will have.

Straits Primary School recognises that moving to a cloud based solution raises a number of 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: ParentHub secure identity server encrypts user access credentials that are required to access ParentHub.

  A username and password must be entered to access any part of ParentHub. Each user requires a unique username and password. In the event an account is compromised the school is able to deactivate the affected account. The school can choose which staff are

able to access ParentHub and assign different roles to those staff members, thus managing which staff have access to the data within ParentHub

Access to the infrastructure is restricted via VPN access which is only allocated to required personnel via Active Directory and requires multi factor authentication.

- **ISSUE**: Transfer of data between the school and the cloud
  RISK: Risk of compromise and unlawful access when personal data is transferred
  MITIGATING ACTION: To protect data in transit between ParentHub servers and the web browsers/mobile devices that run the ParentHub application, Secure Sockets Layer (SSL)/Transport Layer Security (TLS 1.1 and above) is used to create secure tunnel protected by 256-bit Advanced Encryption Standard (AES) encryption. Data in the ParentHub database is encrypted at rest using 256-bit Advanced Encryption Standard (AES) encryption

- **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: ParentHub stores its data within Microsoft's Azure cloud infrastructure. This utilizes automatic 'scale up' features within Microsoft's Azure cloud platform. This means that the service remains resilient even under the heaviest load. ParentHub guarantees 99.9% uptime during school hours (08:00 to 16:00). To date ParentHub has not dropped below 99.9% uptime

- **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 compliant with EU Data Protection Law
  MITIGATING ACTION: ParentHub is located within the EU and so all ParentHub data is stored within the EEA. As described in ParentHub's Sub Processor Policy, some data is transferred to the USA when e-mails are sent via ParentHub service or when support requests are submitted to support@parenthub.co.uk. All data shared with third parties in the USA is done under the EU-US Privacy Shield initiative

  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.

ParentHub's transfer of data outside the European Union to SendGrid and Zendesk is covered by Standard Contractual Clauses.

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: ParentHub will never share the personal data of its users with a third party, unless permission of the data subject is provided for the sharing with that specific third-party

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: When a school requests its data to be deleted, ParentHub, unless prohibited to do so by law, will delete the data. However, even after deletion, all information will continue to exist for a period of time in two forms: (1) in ParentHub's database backups for a period of no longer than 35 days from the date data is deleted; and (2) in ParentHub's server logs for a period no longer than 90 days from when the data was logged

- **ISSUE:** Data Back ups
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Continuous backups are taken to ensure service continuity in the event of any system failure or data loss. ParentHub's main database and all backups are encrypted at rest

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Low-level auditing software is run on all production systems to record potentially malicious actions that may take place. If ParentHub become aware of a security breach of users' Personal Data, ParentHub will notify affected users as required by applicable laws and may post a notice on the Services as required by applicable laws. ParentHub run regular vulnerability scans on its systems and ParentHub's office network using a trusted third party

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The UK has an approved Adequacy Agreement with the EU and therefore post Brexit Evidence for Learning will continue to remain compliant with the provision of cloud storage held within the EU. This means that the school remains GDPR compliant when using ParentHub services

- **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: Any data subject can request a copy of the data that ParentHub hold about them by e-mailing support@parenthub.co.uk. Subject Access Requests will generally be fulfilled within 30 days

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The school remains the data controller for any data shared by the school to ParentHub. If data needs to be added, deleted or updated, this is done by the school using their management information system. This means that ParentHub use the data to carry out a specific function on behalf of the school, i.e. sending school messages to parents. ParentHub will never add, delete or update any of the school's data unless the school specifically requests ParentHub to do so. ParentHub is the data controller for the data that does not belong to the school, which includes the information that is entered when a person creates an account in the ParentHub services

- **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: ParentHub stores its data within Microsoft's Azure cloud infrastructure which is managed in compliance with multiple regulations, standards and best-practices, including ISO/IEC 27001, ISO/IEC 27018, SOC 1, SOC 2 and UK G-Cloud

The ParentHub service is geo-redundant, which means it runs in multiple locations at once. This means that a failure in one service location would not affect the running of the service. Only in the event of multiple failures in disparate locations may the service be affected

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

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Personal information used in the 'ParentHub' platform is always kept to a minimum and is only visible by staff elected by the school. ParentHub 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 actions of all ParentHub users (staff and parents) are logged to ensure that an audit trail is available. ParentHub also use internal monitoring and auditing of its employees who are able to access data within the ParentHub system

Describe the purposes of the processing:

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

1. Scaleability
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

Consider how to consult with relevant stakeholders:
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:

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)

ParentHub will only process personal data that is necessary to run the service. Personal data is never shared with any other third-party

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. Accredited to ISO 27001/27018 and UK G-Cloud	Reduced	Medium	Yes
Data Breaches	ParentHub'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

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Paul Freear	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	YourIG	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 ParentHub 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 If overruled, you must explain your reasons		
Comments: N/A		
Consultation responses reviewed by: N/A If your decision departs from individuals' views, you must explain your reasons		
Comments: N/A		
This DPIA will kept under review by:	Paul Freear	The DPO should also review ongoing compliance with DPIA