Data Protection Impact Assessment (ParentPay)

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. St. Mary's CE (VC) Primary School operates a cloud based system called ParentPay. As such St. Mary's CE (VC) 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.

St. Mary's CE (VC) Primary School recognises that moving to a cloud service provider has a number of implications. St. Mary's CE (VC) 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 GDPR is satisfied by the school.

St. Mary's CE (VC) 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.

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? – To help deliver a cost effective solution to meet the needs of the business. The cloud based system will enable the school to manage cashless payments when delivering services to children. ParentPay is a payment platform enabling parents to securely pay for school items online at a time convenient for them. ParentPay offers: ▪ A cashless till integration for schools ▪ A stand alone flexible cashless solution for schools ▪ It can provide a management information system/attendance option ▪ Parents can see full meal information online ▪ Schools can also manage school trips and clubs, wraparound care, holiday clubs, etc ▪ The school through ParentPay can send payment alerts or school messages by text or e-mail to parents ParentPay includes a communication system so the school office can easily send out important information and updates to parents. In terms of communication 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 ParentPay 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. If this facility is used by the school, 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 St. Mary's CE (VC) Primary School Privacy Notice (Pupil).

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

ParentPay can be accessed by the user via mobile devices.

St. Mary's CE (VC) 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

ParentPay 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: 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 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 considered the lawful basis by which it processes personal data. This is recorded in St. Mary's CE (VC) Primary School Privacy Notice (Pupil). In establishing the lawful basis, the school needs to determine which one 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. ParentPay may collect information from online contact forms, import of data from the school management information system, verbal and/or written information from the 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? – St. Mary's CE (VC) 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, the school's management information system 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: 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 and their school groups – classes, years, etc). The Privacy Policy for ParentPay states that the following personal data will be collected: *Students:* The first and last names of the student. Date of Birth. Gender. School groups (classes, years etc.). Dietary requirements, home address, and admission number. History of pupil's meal selection. Trip information *(if ParentPay is used for this purpose within the school setting)*. This will also include emergency contact details, medical details, dietary requirements, doctors contact details, EHIC and passport (if appropriate). *Parents:* The first and last name of the parents/guardians/carers. Their username and password. Gender, home address, daytime telephone number, home telephone number and mobile telephone number. E-mail address. Payment history and balances. Payment card details. *Staff:* First and last name. Gender. The school will ensure that it has the authority to share data with ParentPay on behalf of the school; it has obtained the lawful basis to provide the personal information of any individual to ParentPay and have obtained all necessary consent to contact any individual through the Services (via the ParentPay application, or by email or SMS).

ParentPay's collection of only data that is necessary to support the service supports the 'data minimization' principle. ParentPay 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 ParentPay.

The information is sourced from St. Mary's CE (VC) Primary School from the management information system either via manual import or automated transfer.

Special Category data? – Some of the personal data collected may fall under the GDPR special category data. This includes dietary information which may relate to a student's religion; or the issue of allergies and health.

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? – The school will 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? – How many individuals are affected (pupils, workforce, governors, volunteers)? And what is the geographical area covered? Reception and Year 1 to Year 6 pupils 217 and workforce 36.

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? – St. Mary's CE (VC) 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) St. Mary's CE (VC) 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? – ParentPay users (students, parents, staff) may have individual user accounts to log into ParentPay to retrieve communications. These accounts are accessible to individual users via a unique username and password.

Do they include children or other vulnerable groups? – Some of the data is classified under GDPR as special category. This includes data relating to health and religion and dietary requirements. However, personal data will be collected: pupil information including the pupil name, pupil UPN (unique pupil number), their home address, date of birth, gender, and pupil class name.

Are there prior concerns over this type of processing or security flaws? – Data Controller data is encrypted at rest and is transmitted using HTTPS between client machines and ParentPay servers. TLS 1.1 and above is implemented to ensure that data is encrypted during transit

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

ParentPay has a dedicated information security team who use a suite of tools including intrusion detection systems, network monitors and vulnerability scanners to carry out regular checks on the infrastructure and to identify and alert us to any vulnerabilities or breaches

St. Mary's CE (VC) Primary School has the responsibility to consider the level and type of access each user will have.

St. Mary's CE (VC) 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: ParentPay secure identity server encrypts user access credentials that are required to access ParentPay. A username and password must be entered to access any part of ParentPay. 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 ParentPay and assign different roles to those staff members, thus managing which staff have access to the data within ParentPay

- **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 ParentPay servers and the web browsers/mobile devices that run the ParentPay 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 ParentPay database is encrypted at rest using 256-bit Advanced Encryption Standard (AES) encryption

- **ISSUE:** Use of third party sub processors?
  RISK: Non compliance with the requirements under GDPR
  MITIGATING ACTION: ParentPay use a range of trusted service providers to help deliver its services. All of their suppliers are subject to appropriate safeguards, operating in accordance with ParentPay's specific instructions and limitations, and in full compliance with Data Protection Law

  All ParentPay third party suppliers are required to sign and agree to a data processing agreement and a non-disclosure agreement. This agreement ensures that only the necessary data is provided and is exclusively used and held for processing to provide the required functionality to ParentPay

  Third parties based outside of the European Economic Area (EEA) have contractual clauses included into their DPA's as recommended by the ICO to ensure compliance with the GDPR

- **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: ParentPay 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. Praent Pay guarantees 99.9% uptime during school hours (08:00 to 16:00). To date ParentPay 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: ParentPay is located within the EU and so all ParentPay data is stored within the EEA. As described in ParentPay's Sub Processor Policy, some data is transferred to the USA when e-mails are sent via ParentPay service or when support requests are submitted to support@parentpay.co.uk. All data shared with third parties in the USA is done under the EU-US Privacy Shield initiative

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: GDPR non-compliance
  MITIGATING ACTION: ParentPay 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: GDPR non-compliance
  MITIGATING ACTION: ParentPay will only retain information for as long as is necessary to deliver the service safely and securely. ParentPay may need to retain some records to maintain compliance with other applicable legislation – for example finance, taxation, fraud and money laundering law requires certain records to be retained for an extended duration, in some cases for up to seven years

  Pupil data will typically be removed or anonymised when the following rules are met: (1) The pupil has been archived by the School for longer than one month. (2) The pupil does not have any meal consumption or attendance data within the last 13

months. (3) The pupil has not received a payment for any payment item within the last 13 months. (4) The pupil balance is zero

Payer (Parent) data will usually be removed or anonymised when the following rules are met: (1) They have not logged in for 13 months. (2) They have not topped up or spent within the last 13 months. (3) Parent balance is 0 (zero), and all pupil balances are 0 (zero). (4) There are no active pupils associated with the account

Personal information in trip records will be removed 1 month after trip completion (if applicable to the school setting)

- **ISSUE:** Data Back ups
  RISK: GDPR non-compliance
  MITIGATING ACTION: Back ups of the ParentPay databases are taken on a regular basis. These are secured and encrypted to ensure that personal data is protected against accidental destruction or loss while hosted. Full database backups are usually tested on a monthly basis

- **ISSUE:** Responding to a data breach
  RISK: 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 ParentPay become aware of a security breach of users' Personal Data, ParentPay will notify affected users as required by applicable laws and may post a notice on the Services as required by applicable laws. ParentPay run regular vulnerability scans on its systems and ParentPay's office network using a trusted third party

- **ISSUE:** No deal Brexit
  RISK: GDPR non-compliance
  MITIGATING ACTION: The ParentPay primary and backup infrastructure is located within the United Kingdom

  ParentPay is keen to ensure parties are protected and that our supply contract(s) remain compliant with prevailing data protection legislation. In the event of a Brexit condition – be that with an agreement, or a 'no-deal' scenario:

  ParentPay will still be processing personal information of EEA data subjects, and so are required by law to comply with the regulation. Additionally, the Data Protection Act (2018) is UK law, and this is now aligned with the GDPR

It is possible that in a 'Brexit' scenario, the UK may be considered as a 'third country', and may not hold an 'adequacy decision' (Ref: Chapter V – GDPR, Article 44-50)

For this reason, under such circumstances, ParentPay would include the EU approved Model Contract Clauses as an addendum to the ParentPay product Terms and Conditions/Data Processing Agreement

This is considered to be an 'appropriate safeguard' under Data Protection Law

The ParentPay Privacy Notice will also be updated to reflect the use of these safeguards

- **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: ParentPay's Privacy Notice documents the rights of data subjects to access their personal data under data protection law

- **ISSUE:** Data Ownership
  RISK: GDPR non-compliance
  MITIGATING ACTION: The school remains the data controller for any data shared by the school to ParentPay. If data needs to be added, deleted or updated, this is done by the school using their management information system. This means that ParentPay use the data to carry out a specific function on behalf of the school, i.e. sending school messages to parents. ParentPay will never add, delete or update any of the school's data unless the school specifically requests ParentPay to do so. ParentPay 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 ParentPay 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: ParentPay 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 ParentPay 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:** GDPR Training
  RISK: GDPR non-compliance
  MITIGATING ACTION: Appropriate training is undertaken by personnel that have access to ParentPay

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

  ParentPay is certified Security Essentials Plus and ISO 27001 complaint

  ParentPay are certified PCI DSS Level 1 merchant which subjects ParentPay to an annual audit by a third party qualified security assessor (QSA). A complete audit trail of all payments can be securely maintained. Transaction references and identifiers link parent and school accounts to the payment and banking network

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: 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: 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) ParentPay 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

18

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
No deal Brexit	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 Security Essentials Plus and ISO 27001	Reduced	Medium	Yes
Data Breaches	ParentPay's ability to respond and deal with a data breach	Reduced	Low	Yes
No deal Brexit	Servers located in the UK	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:	**[Insert name]**	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	**[Insert name]**	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 security measures are in place? Is data on ParentPay servers encrypted at rest, dual authentication, enterprise level permissions? *(2)* Where are the servers located which store ParentPay data? *(this determines applicable data protection law)* *(3)* What accreditation does ParentPay have? *(ISO 27001, etc)* *(4)* Security of personal data from the school to ParentPay servers? What level of encryption is applied? (5) Security in terms of use of third party suppliers? (6) What data backups take place? (7) Contingency arrangements around a no deal Brexit		
DPO advice accepted or overruled by:	Yes	If overruled, you must explain your reasons
Comments:		
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:	**[Insert name]**	The DPO should also review ongoing compliance with DPIA

23