ico.
Information Commissioner's Office

Data Protection Impact Assessment (Teachers2Parents)

Gig Mill Primary School operates a cloud based system. As such Gig Mill 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.

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

Gig Mill 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 3

Step 2: Describe the processing 7

Step 3: Consultation process 12

Step 4: Assess necessity and proportionality 12

Step 5: Identify and assess risks 13

Step 6: Identify measures to reduce risk 14

Step 7: Sign off and record outcomes 15

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. Teachers2Parents provides an online platform which enables communication by text and email with the addition of a two-way app messaging service. Schools can send out messages to parent groups at no charge. Parents will receive these messages in the app. Teachers2Parents has the following components:

Texts to Parents – Teachers2Parents provides a platform for the school to contact parents and guardians efficiently using SMS directly to their mobiles. The school can also send messages in bulk to a whole class, form or group. Messages can be scheduled in advance by the school.

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 Teachers2Parents 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 Gig Mill Primary School Privacy Notice (Pupil).

MIS Integration

Teachers2Parents uses an Application Program Interface with the school's management information system to share school data. Xporter on Demand provides a fully accredited and secure interface for the school to use on demand.

Xporter on Demand automatically updates to the latest version and provides the school with the functionality to opt in or out of the data that the school wished to share with Teachers2Parents.

Wonde and Third Party Apps/Vendors

Wonde's core service is used by a large percentage of schools in the UK to control the Management Information System (MIS) data it shares with third party vendors used at the school. These vendors include solutions for assessment, maths, English, library management, parent communications, parent payments, Multi Academy Trusts, voucher systems, Google/Microsoft syncing, classroom content providers etc.

Wonde is ISO27001 accredited and the majority of schools use Wonde to manage their MIS data sharing and syncing with multiple third party vendors. An overview of how schools do this can be found here https://www.wonde.com/school-data-management.

When a vendor (app), or vendors, requests to be connected to a school via Wonde - if the school approves that vendor(s) request and for Wonde to facilitate it, then Wonde will complete a base integration with the schools' MIS.

Wonde request (but do not extract) the permissions that are required for the majority of vendors that use its services. Wonde will then only extract and send data that has been approved by a school to send onwards to their chosen vendors. For clarity, Wonde does not extract data that is not approved by the schools for the vendors they are using.

Gig Mill Primary School can reduce the requested Wonde permissions upon the integration taking place, and Wonde can assist schools with this. Gig Mill Primary School also has the ability to change the permissions whenever it likes, but in doing so ensures that it has considered how that may affect its use of approved vendors (i.e. the flow of data to those vendors via Wonde for the vendors to provide the agreed service).

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

Teachers2Parents 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 lawful basis of why the school collects pupil data. Specifically this relates to The Children Act and subsequent amendments, The Education Act and subsequent amendments and The Childcare Act 2006 and subsequent amendments.

How will you collect, use, store and delete data? – The information collected by the school is retained on the school's management information system. Teachers2Parents also collects information which is sourced 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? – Gig Mill 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, Integris G2 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? – Teachers2Parents holds information from customer schools about both pupils and employees for the purpose of providing a service in accordance with the terms and conditions for contracted services. This information is held and processed in compliance with the General Data Protection Regulation (GDPR).

The customer school remains the 'Data Controller' in respect of pupil data at all times. As such the school is obliged to ensure that the information provided is accurate and up-to-date. As part of the school's obligation as 'Data Controller', it must have identified a lawful basis to collect pupil personal data.

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

Special Category data? – Data revealing health, racial or ethnic origin, and religious beliefs are collected by the school in its Management Information System. This may be communicated via Teachers2Parents. The lawful basis for collecting special category information relates to Article 9 2 (g) *processing is necessary for reasons of substantial public interest and is authorised by domestic law.*

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

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? – Gig Mill 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) Gig Mill 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? – Teachers2Parents users (students, parents, staff) may have individual user accounts to log into Teachers2Parents to retrieve communications. This may be via the Teachers2Parents app.

Do they include children or other vulnerable groups? – All of the data will relate to children.

Are there prior concerns over this type of processing or security flaws? – Gathers only data required to operate Teachers2Parents from the school MIS system. Extracted data is then encrypted prior to transmission to the Teachers2Parents system. Data is transmitted in an encrypted form.

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

Gig Mill Primary School recognises that moving to a cloud based solution raises a number of General Data Protection Regulations issues as follows:

Are there prior concerns over this type of processing or security flaws? – All data is encrypted in Teachers2Parents. Data transfer is secured by TLS 1.2.
Gig Mill 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: Teachers2Parents implement 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 Teachers2Parents 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: Teachers2Parents 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

- **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 encrypted at rest and in transit (TLS 1.2 for e-mails) and encryption at rest is Bitlocker

- **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: The servers hosting Teachers2Parents are located within the EU. The servers are UK based with AWS (Amazon Web Services)

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Teachers2Parents is an ICO registered company, fully compliant with UK GDPR data security handling and reporting. 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)

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
- **MITIGATING ACTION:** Teachers2Parents is fully compliant with UK GDPR data security retention and storage. Teachers2Parents has data deletion functionality

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Teachers2Parents 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: Teachers2Parents has the functionality within the reports menu to handle and respond to Subject Access Requests. The procedure is noted in Teachers2Parents (Eduspot) Data Protection Agreement

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The school remains the data controller. Teachers2Parents (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: Teachers2Parents 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 School Pod 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 Teachers2Parents

- **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: Teachers2Parents 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

  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:

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. 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:

The lawful basis for processing personal data is contained in the school's Privacy Notice (Pupil). The lawful 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, with firewall, VPN and encryption technologies	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:	Gig Mill Primary School	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Gig Mill Primary School	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 Accepted/Headteacher If overruled, you must explain your reasons		
Comments:		
Consultation responses reviewed by: Headteacher If your decision departs from individuals' views, you must explain your reasons		
Comments:		
This DPIA will kept under review by:	School Business Manager	The DPO should also review ongoing compliance with DPIA