Data Protection Impact Assessment (School Life - Comms)

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. Old Park School operates a cloud based system called School Life. As such Old Park 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.

Old Park School recognises that moving to a cloud service provider has a number of implications. Old Park 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. Old Park 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? – 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.

School Life is first and foremost a communication platform, helping schools share and retrieve information. School Life 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 School Life 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 Old Park School Privacy Notice (Pupil).

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

Old Park 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 School Life 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

School Life 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 highlighted consent as the lawful basis by which it processes personal data. This is recorded in Old Park School Privacy Notice (Pupil).

How will you collect, use, store and delete data? – The information collected by the school is retained on the school's management information system. School Life 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? – Old Park 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: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

What is the nature of the data? – Pupil data relates to personal identifiers and contacts (such as name, unique pupil number, contact details and address). The Privacy Policy for

School Life states that the following personal data will be collected: pupil information including the pupil name, pupil UPN (unique pupil number), pupil class name.

Parental/guardian information will be collected relating to Parent/Guardian name, parent/guardian e-mail address, and parent/guardian contact number.

It also states under the 'data minimization' principle that School Life 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 School Life.

The information is sourced from Old Park 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? – The school will consider the data retention period as outlined in the IRMS Information Management Toolkit for Schools

Scope of data obtained? – How many individuals are affected (pupils, workforce, governors, volunteers)? And what is the geographical area covered? Reception and Year 1 to Year 14 pupils [149], and workforce [157].

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? – Old Park 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) Old Park 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? – School Life users (students, parents, staff) may have individual user accounts to log into School Life 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 School Life servers are encrypted. Log in to the School Life portal is via a strong SHA-2/2048 bit encryption. School Life uses Amazon Web Services which is certificated to certain security and regulations including ISO 27001 and PCI Data Security Standard.

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

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

Old Park 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: The School Life administration system can only be accessed via authenticated users that have been granted the role of staff members. Only existing staff members or School Life administrators can grant this level of authorization. User passwords are not stored in the system – one way cryptographic hash is created in their place

- **ISSUE**: Transfer of data between the school and the cloud
  RISK: Risk of compromise and unlawful access when personal data is transferred
  MITIGATING ACTION: Access at server level is restricted to senior members of staff and are only accessible across a secure VPN who ensure that the lasts patches updates are installed. All data kept on the School Life database servers are encrypted, whilst login to the School Life portal is via strong SHA-2/2048 bit encryption

- **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: Amazon EC2 cloud infrastructure is certified to certain security and regulations including ISO 27001 and the PCI Data Security Standard. All School Life servers are located behind firewalls and only ports and services that are deemed necessary are opened

- **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: School Life uses Amazon EC2 to host School Life servers, which in turn hosts the personal data which is uploaded from the school. School Life would keep the school's data on its systems for as long as a relationship exists between the school and School Life

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: School Life's Privacy Notice states that the school, and for that matter the parent/guardian, has a right to access any personal information that School Life processes including what personal data is held, the purposes of the processing, categories of personal data concerned, recipients to whom the personal data has/will be disclosed, how long School Life stores the information, and information about the personal data source. If School Life receives a request from the school to exercise any of these rights, School Life may ask the school to verify it's identity before acting on the request; this is to ensure that the data is protected and kept secure

  As part of its commitment to privacy and security, when a school contacts the support desk, schools will be asked to confirm specific details to confirm that it is a genuine call/request. School Life will always assist schools, where possible, in meeting their obligations under UK GDPR

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The personal data will be managed in line with the school's data retention policy. School Life only ever retains personal information for as long as is necessary. School Life actively reviews its Privacy Policy to meet these obligations. School Life will keep school data on its systems for as long as a relationship exists between the school and School Life. Additionally, every entry on the 'School Life' platform will be fully cleansed of content and data within 30 days of the contract with the particular school ending

- **ISSUE:** Data Back ups
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: School Life use Amazon Web Services (AWS) back up services. AWS back up is a fully managed, policy based back up solution that makes it easy to automatically back up the School Life application data across AWS services in the cloud

  AWS back up's policies provide automated backup scheduling, back up retention management, and lifecycle rules, which assists in streamlining back up processes. AWS backup supports backing up EBS volumes, RDS databases, DynamoDB tables, EFS file

systems, and Storage Gateway volumes and stores School Life back up data durably and securely using Amazon S3. AWS back up's centralised back up monitoring, back up encryption, and back up access policy features help School Life to meet internal and regulatory backup compliance requirements

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance

  MITIGATING ACTION: The system has passwords for every School Life staff member. Data breaches can be dealt with by any member of staff as a result. Every member of School Life staff is trained in how to shut down the system if required whilst any data breach is dealt with. Every member of staff has signed a confidentiality agreement. Passwords are changed every three months automatically and are alpha numerical. They are not recorded on any file. All accesses to the system from School Life staff or school side are logged and stamped with date and time. All School Life staff are trained in how to deal with data breaches and a written policy and procedure exists

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: School Life use Amazon S3 to host its database and related programs. The data is currently stored on servers in Eire. Servers are also based on the UK mainland and can be switched post Brexit

- **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: School Life have a written data Subject Access Request policy and procedure. School Life staff are trained in what to do when a request comes in. SARs are managed the UK GDPR data manager, or in their absence, by two deputies on behalf of the school

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: School Life does not share or disclose any of the school's personal information without the school's consent. School Life uses third parties to provide the service, e.g. Amazon EC2 for storing data in the cloud. However, all

processors acting on the behalf of School Life only process school data in accordance with instructions form School Life and in compliance with School Life's Privacy Notice, data protection law, and any other appropriate confidentiality and security measures

- **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: This should be monitored to address any changes in technology and its impact on data to enable UK GDPR compliance

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

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Personal information used in the 'School Life' platform is always kept to a minimum and is only visible by staff elected by the school. School Life 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

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)

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 and PCI Data Security Standard	Reduced	Medium	Yes
Data Breaches	School Life'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:	Miss Tina Partridge	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Miss Tina Partridge	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 School Life 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:

YourIGDPO Service liaised with supplier for further clarification as outlined above in summary of DPO advice.

Consultation responses reviewed by: Retrospective

If your decision departs from individuals' views, you must explain your reasons

Comments:

This DPIA will kept under review by:	Miss Tina Partridge	The DPO should also review ongoing compliance with DPIA