Data Protection Impact Assessment (Evidence for Learning)

Old Park School operates a cloud based system, called Evidence for Learning (the owners are the TeacherCloud Ltd). Access to Evidence for Learning is through the internet. Resources are retrieved from Evidence for Learning via the Internet, through a web-based application, as opposed to a direct connection to a server at the school. Access to Evidence for Learning can be through PC, smartphone, iPad and tablet. 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 using a cloud based system 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 server 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 a review of 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? – Evidence for Learning (EfL) is an online learning journey which allows teaching staff to evidence and track pupil progress. Teaching staff can take videos/photographs, link these to a child, add a written observation and link the piece of evidence to different assessment frameworks.

Parents and carers are able to log into the parent portal to see evidence for their child. EfL is accessed by class based IPads and desktop computers.

Old Park School luse the following personal information; Full name, date of birth, class, gender, ethnicity, Free School Meals (FSM), Looked After Children (LAC), parent name, parent email.

The information will be used to inform the school's assessment of its children evidencing and tracking progress against individual learning intentions and targets related to Education Health & Care (EHC) Plans.

Evidence for Learning enables teaching staff to amend and add to these goals over time in order to respond to a learners' ongoing needs and development.

Evidence for Learning enables parents/carers to capture and submit their own photos, videos and notes to reflect the learner's development and experiences at home and outside in the community.

Evidence for Learning will assist the school in the following ways:

- Demonstrate impact and show what learners can do as a result of the school's curriculum, pedagogy and support
- Assess against any curriculum framework including custom-built frameworks
- Evidence, assess and track progress against individual targets related to EHC Plans using Old Park School assessment model and schemes
- Automatically link evidence, achievements, outcomes and judgements

- Tools for working with and assessing the 5 areas of engagement in line with DfE requirements and guidance
- Report and analyse assessment and evidence data
- Old Park School lis in a more informed position to assist in planning, assessment and reporting
- Improved engagement and involving parents in their child's learning and development
- Systemise assessment and moderation

The features of Evidence for Learning include:

- Working with the school's customised assessment criteria and sets of individualised targets. Individualised learning plans, EHCPs, progression frameworks and/or accreditation
- Frameworks can be edited and adapted over time to reflect the needs of learners
- The ability to record small and subtle improvements: photo/video/audio, notes judgements all linked to targets
- Creation of Assessment Books using the school's assessment schemes or commonly used assessment models such as MAPP. Evaluate using the 5 areas of engagement (DfE, Jan 2020)
- Ability to build a learner profile for each pupil containing all evidence, notes and assessments relevant to their learning and development
- Report and analyse assessment and evidence data – formative and summative assessment
- Generate rich learning journeys in an instant
- Share and engage with parents via the Evidence for Learning secure parent portal. Additionally, parents/guardians can submit evidence

The use of Evidence for Learning will also enhance the educational experience, deliver a cost effective solution, and help meet the needs of the school. The school will be complying with Safeguarding Vulnerable Groups Act, KCSiE guidance, 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 Evidence for Learning the school aims to achieve the following:

1. Scaleability
2. Reliability
3. Management
4. Delivery at a potentially lower cost
5. Supports mobile access to data securely
6. Update of documents in real time (where applicable)
7. Good working practice, i.e. security of access

Evidence for Learning is a web based application which uses personal data to set up individual log ins.

Evidence for Learning cannot do anything with the school's data unless they have been instructed by the school. The schools Privacy Notice will be updated with reference to Evidence for Learning. The school is the data controller and Evidence for Learning is the data processor.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

The Privacy Notices (Pupil) for the school provides the lawful basis of why Old Park 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) for the purpose named above in accordance with the legal basis of Legal Obligation.

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.

In terms of processing special category data, the following will apply:

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.*

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 computer systems. Evidence for Learning set-up requires a parent/guardian e-mail address to give access to the app. E-mail accounts are required for each parent/carer. 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. Pupil information also includes classroom work, assessments and reports.

Parental/guardian information is obtained by the parent/guardian providing personal data relating to pupil name, their relationship to the child, first and last name of the parent/guardian, and e-mail address.

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, Management Information Systems and various third party Information Society Services applications including Evidence for Learning.

However, concerning Evidence for Learning only staff working at Old Park School can see all of the children's Learning Journeys. No information from Evidence for Learning can be shared with other people without explicit consent of the parents/guardians of those children. Photographs or videos from Evidence for Learning cannot be posted on any social networking site or displayed in a public place (even if they are only about the child of the parent/guardian).

What types of processing identified as likely high risk are involved? – Transferring of 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 full name, date of birth, class, gender, ethnicity, FSM provision, whether LAC and the name of the parent/guardian and the parent/guardian e-mail address).

The Privacy Notice (Pupil) for Evidence for Learning states during normal use of the App, evidence photos, videos and data are transmitted from the app to a secure data centre. All data transfer between a user's device and Evidence for Learning data centres in the cloud is encrypted and is done securely via https using SSL.

The data stored in Evidence for Learning data centres is used for no other purpose than to provide the services available in the App.

Staff are constantly observing and assessing the children in their care. Old Park School takes photographs and videos as evidence of the child's achievements and experiences. The

school then use these to assess and monitor each child's progress and identify areas for development.

A Learning Journey is a record of each child's learning and shows snap shots of children's achievements and progress in relation to individual learning intentions and targets related to Education Health & Care (EHC) Plans, etc.

Not every activity a child does will be recorded, staff will focus on significant moments in each child's learning.

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

Evidence for Learning will be regularly monitored by the Senior Leadership Team.

Special Category data? – Some of the personal data collected falls under the UK GDPR special category data. When capturing images of the child this will identify the race; ethic origin; and health.

Data revealing racial or ethnic origin, and religious beliefs may be collected by the school and contained in Evidence for Learning. 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 each pupil enrolled at Old Park School. Parents/guardians will only be able to view their

own child's information. Parents/guardians will set up an e-mail address, secure password and PIN number to be able to access their child's information only.

Parents/guardians will have access 24 X 7 to their child's Learning Journey.

Parents/guardians can view and contribute to their own child's Learning Journey, receiving a new e-mail whenever a new observation is added to the child's Learning Journey.

Parents can leave a reply/comment on the observations made by staff.

Parents can add their own observations/comments and photos/videos from things their children do at home.

How long will you keep the data for? – When children leave Old Park School a copy of their learning journey may be transferred electronically and securely and passed onto the Parents/Carers. The pupils account will be deleted, and a sample of the child's learning journey may be stored in line for a limited period for Ofsted and stored securely.

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 (Pupil). And what is the geographical area covered? 148 within the school.

Evidence for Learning will be used to record a child's learning and achievements. It will not be used as a tool for general communication between Old Park School and home and will not be monitored on a daily basis.

However, staff will check regularly for parent replies/comments.

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 parents to manage the parent/pupil relationship.

Through the Privacy Notice (Pupil) 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? – Personal data is collected for each pupil enrolled at Old Park School. Parents/guardians will only be able to view their own child's information. Parents/guardians will set up an e-mail address, secure password and PIN number to be able to access their child's information only.

Parents/guardians will have access 24 X 7 to their child's Learning Journey.

Parents/guardians can view and contribute to their own child's Learning Journey, receiving a new e-mail whenever a new observation is added to the child's Learning Journey.

Parents can leave a reply/comment on the observations made by staff.

Parents can add their own observations/comments and photos/videos from things their children do at home.

The school will be able to upload personal data from its PC for the data to be stored remotely by a service provider. Any changes made to files are automatically copied across and immediately accessible from other devices the school may have.

Do they include children or other vulnerable groups? – Personal data will relate to children who are particularly vulnerable. By undertaking this Data Protection Impact Assessment Old Park School is ensuring that appropriate data protection safeguards are in place.

Are there prior concerns over this type of processing or security flaws? – Does the third party app provider store the information in an encrypted format? What is the method of file transfer (if applicable)? For example, the most secure way to transfer is to encrypt the data before it leaves the computer.

Old Park School recognises that moving to a cloud based solution raises a number of UK General Data Protection Regulations issues as follows:

- **ISSUE:** Evidence for Learning will be storing personal data including special category information.
  RISK: There is a risk of uncontrolled distribution of information to third parties.
  MITIGATING ACTION: Evidence for Learning control access through passwords. Passwords cannot be seen

  Storage and processing is carried out on computers and networks provided by Amazon Web Services (AWS) as a sub-processor. Evidence for Learning have configured it's environments to use VPC networks with robust security groups controlling access. Evidence for Learning ensure all of the software used is up to date and fully tested, encrypting school data on Evidence for Learning servers and the connections between the school and servers

  Evidence for Learning User Manager tool forces a strong Password Policy containing a mix of uppercase, lowercase, numeric and special characters. User passwords are salted and hashed using SHA512 encryption. Evidence for Learning User Manager supports two-factor authentication (2FA)

  Evidence for Learning cloud infrastructure hard disks are encrypted, all data is encrypted at rest

- **ISSUE**: Transfer of data between the school and the cloud
  RISK: Risk of compromise and unlawful access when personal data is transferred
  MITIGATING ACTION: Connection between Old Park School and the Evidence for Learning servers are encrypted. Evidence for Learning cloud infrastructure hard disks

are encrypted, and all data is encrypted at rest. Evidence for Learning use SSL/TLS 1.2 security at the network level to ensure all data is encrypted in transit

- **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: Data is stored within data centers in the EU

  Your Cloud Administrator has a password to maintain the school's system data stored in the Cloud. Cloud data is protected with class-level and object-level Access Control Lists (ACLs). Evidence for Learning routinely conduct 3rd party security audits to verify the security and integrity of its systems and internal controls

- **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: Evidence for Learning services are configured as autoscaling, load-balanced, resilient environments, each configured across multiple geographically distributed availability zones

  This ensures high levels of uptime and performance. Evidence for Learning have configured its environments to use VPC networks with robust security groups controlling access

- **ISSUE:** Data Retention
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Data will be removed within 30 days of receiving request. At the end of a contract, leaving customer data is made inaccessible within 7 days and deleted from the cloud after 90 days. The deletion of data will then be fully completed within 30 days. This gives customers time after contract end to retrieve their data. Once

Evidence for Learning have completed the deletion process, they will notify the school in writing to confirm

I

- **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: The school can respond to Subject Access Requests by obtaining relevant personal data to fulfil the request

  In exercising data subject access rights, the school can correct or delete its data that is stored within the software by Evidence for Learning, without the need to contact or involve the company directly. The school can also contact Evidence for Learning to correct or delete data on behalf of the school

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The school as data controller maintains ownership of the data. Evidence for Learning is the data processor. In terms of disclosure Evidence for Learning will not release the information to any third party unless the request is subject to legal obligation without obtaining the express written authority of the school who provided the information

- **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 Evidence for Learning services

- **ISSUE:** Lawful basis for processing personal data
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: School has included Evidence for Learning in its Privacy Notice (Pupil) which identifies the lawful basis for processing personal data

- **ISSUE:** Responding to a Data Breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Evidence for Learning services are configured as autoscaling, load-balanced, resilient environments, each configured across multiple geographically distributed availability zones

  This ensures high levels of uptime and performance. Evidence for Learning have configured its environments to use VPC networks with robust security groups controlling access

  In the event of a data breach there is an expectation that Evidence for Learning would contact the school and where appropriate report any data breach which meets the threshold to the supervisory authority (ICO)

- **ISSUE:** Third party processor and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: The school is unable to exercise the rights of the individual
  MITIGATING ACTION: Evidence for Learning do not share customer data, except as explicitly requested by the school. Old Park School can provide access to data to its staff, learners and other stakeholders (such as the parents of learners)

  Old Park School and its staff can view, download or print some or all of the data and share it with other staff, parents, government agencies and any other stakeholders at their discretion. the TeacherCloud Ltd, only accesses and processes the data stored by Old Park School in order to provide, troubleshoot or improve the software and service

  Data collected and stored by Old Park School is not used for commercial purposes. Evidence for Learning do not pass on any personal data or metadata for any commercial purpose and Evidence for Learning will not sell or rent any information to any third party for any reason

- **ISSUE:** Data is not backed up
  RISK: UK GDPR non-compliance

MITIGATING ACTION: Evidence for Learning services are configured as autoscaling, load-balanced, resilient environments, each configured across multiple geographically distributed availability zones

This ensures high levels of uptime and performance. Evidence for Learning have configured its environments to use VPC networks with robust security groups controlling access

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

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Evidence for Learning's data centre, Amazon Web Services (AWS), has been independently certified as ISO 27001 compliant

  Evidence for Learning have an internal data access policy that restricts access to personally identifiable information to a limited number of employees with a specific business need (such as for technical support). No customer information is stored on individual employee computers. Evidence for Learning routinely monitor its systems for security breaches and attempts at inappropriate access

  the TeacherCloud staff are DBS/CRB-checked who may access school data only to assist with support queries or maintenance

  Evidence for Learning are registered with the UK Information Commissioner's Office (www.ico.org.uk), as the TeacherCloud Ltd, registration Number ZB240514

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:

- Scaleability
- Reliability
- Resilience
- Delivery at a potentially lower cost
- Supports mobile access to data securely
- Update of documents in real time
- Good working practice, i.e. secure access to sensitive files

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). 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
Post Brexit (GDPR noncompliance)	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, Penetration Testing and Audit	Reduced	Medium	Yes
Post Brexit	Brexit contingency plans to relocate servers to 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:	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)* Does Evidence for Learning provide the technical capability to ensure the school can comply with rights of access and subject access requests *(i.e. rights to request access, rectification, erasure or to object to processing?)* *(2)* Does the functionality exist to enable the school to respond to subject access requests? *(3)* Does the functionality exist to enable the school to apply appropriate data retention periods? *(i.e. the period for which personal data will be stored)* Please see responses embedded in the Issue, Risk and Mitigating Actions log		
DPO advice accepted or overruled by: Yes – Tina Partridge If overruled, you must explain your reasons		
Comments:		
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:	Tina Partridge	The DPO should also review ongoing compliance with DPIA