Data Protection Impact Assessment (ePEP)

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. 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? – ePEP (Electronic Personal Education Plan) is a platform which monitors educational & attendance for looked-after children.

ePEP provides a single sign on solution for schools with access to an online platform which tracks and monitors looked after children's educational progress and outcomes.

The service includes the collection of live attendance data daily or weekly and the collection of termly key stage attainment data. It can interact with social workers, designated teachers, providers, support specialists and parents and carers to work and communicate securely online with the school.

The ePEP platform provides a holistic area to record and measure the child's educational performance, achievements, targets, aspirations, outcomes, concerns and self-well-being. This assists in helping professionals identify and implement interventions for improving educational quality and achieving better outcomes.

There is a Young Persons Portal within ePEP to securely record important events, achievements and to capture bespoke answers to questions set by the Virtual School. Young People can also connect to ePEP Portal via a secure mobile APP which is optional. The ePEP Attendance Collection Service integrates directly into the ePEP and sends external notifications and alerts to attendance officers. This can assist schools when reporting attendance data to the DfE.

ePEP has a Self-Report Builder functionality for schools to use within the platform to assist in analysing data. This application enables professionals to produce tailored reports, configure threshold alerts, conduct data mining, analyse and drill-down on all aspects of collected ePEP and attendance data. Bespoke reports can be automatically generated weekly or shared between colleagues. Individual cohorts, school data, ePEP completion, key-stage results, collected attendance, attainment data can be downloaded.

It is possible for schools to develop Customisable Dashboards to drill-down on key areas of focus and concern with large or individual cohorts. Attainment, progress, ePEP completion, targets, attendance, quality assurance ratings, Look-up tables, drop-downs menus can be edited by the school to analyse the dashboards.

ePEP Features

- ePEP Single Sign-on Cloud-based fully managed secure platform 24/7 access
- Attainment Collection module including academic flight path for all cohorts
- Bespoke Report Builder & Analytic Dashboard for (Real-time reporting)
- Built in secure Broadcasting and Messaging Service including automated reminders
- Young Persons secure interactive portal (Voice of the Young Person)
- Attendance Collection and monitoring/Push-Pull database connectivity
- Pupil Premium Finance Tracker linked accountability to SMART target section
- Quality Assurance section including automatic notification and feedback to teachers
- Automatic Attendance Collection including Parent or Carer Verification
- Early Years, SEND, Post 16, UASC and child focused modules

ePEP Benefits

- Single Sign-on application allowing teachers access to all allocated children
- Improved quality & completion rates for Personal Education Plans
- Internal case management system for greater transparency
- Improved attainment & attendance monitoring and data accountably
- Low-Risk smooth system implementation tried & tested product
- Bespoke analytical reports including VS dashboard for clear visualisation
- Enhancing communication and data sharing with supporting professionals
- Customisable privilege and control panel settings for total policy control
- PEP Builder administration for self-managing questions and additional sections
- Automatic threshold and vulnerability alerts for improved safeguarding

The use of ePEP will help the school to deliver a cost-effective solution to meet the needs of the business.

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. Update of documents in real time
7. Good working practice, i.e. secure access to sensitive files

The school can easily upload personal data to the cloud. The information can be accessed from any location and from 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 and workforce data 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 lawful 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 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.*

The school has considered the lawful basis by which it processes personal data. This is recorded in Old Park School Privacy Notice (Pupil) and where appropriate in Privacy Notice (Workforce).

How will you collect, use, store and delete data? – The information collected by the school is retained on the school's computer systems and in paper files. The information is also stored in the cloud. 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.

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, via 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 'special category' data from the school to the cloud. Storage of personal and 'special category data in the Cloud. However, in terms of using ePEP the use of special category data will be limited to the lawful basis as outlined in the school's Privacy Notice (Pupil).

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, home address). Characteristics (gender, date of birth), Court Order, Education Health Care Plan (EHCP), Looked After Child (LAC)). Pupil Premium details, Progress funding allocations, PEP money, disabilities, learning needs, and attendance.

Special Category data? – Some of the personal data collected falls under the UK GDPR special category data. This includes health. In terms of using ePEP and special category data the lawful basis is:

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.*

Whatever special category data is used the school will ensure that it has a lawful basis to do this and that this is documented in the school's Privacy Notice (Pupil).

How much data is collected and used and how often? – Personal data is collected for all pupils.

How long will you keep the data for? – The school will be applying appropriate data retention periods as outlined in its Data Retention Policy and 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, Year 1 to Year 14 pupils. ePEP will be used by the school to monitor educational & attendance for looked-after children.

The school will act as in accordance with the lawful basis it has for using personal data. This is outlined in the schools Privacy Notice (Pupil).

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 to manage the school and 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? – Access to the files will be controlled by username and password. Cloud Service provider is hosting the data and will not be accessing it. 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? – In terms of using ePEP special category data may be collected to assist in the enrolment process.

Whatever special category data is used the school will ensure that it has a lawful basis to do this and that this is documented in the school's Privacy Notice (Pupil).

Are there prior concerns over this type of processing or security flaws? – Does the cloud provider store the information in an encrypted format? What is the method of file transfer? For example, the most secure way to transfer is to encrypt the data before it leaves the computer. Encryption does have its limitations inasmuch as the encryption key will need to be shared with others to access the data.

Old Park 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: eGov Solutions Ltd are currently ISO27001 certified, and they undertake to maintain this certification for the Licence Term.

  ISO27001 certification demands best in class controls across: Information security policies, organisation of information security, human resource security, asset management, access control, cryptography, physical and environmental security, operations security, communications security, system acquisition, development and maintenance, supplier relationships, information security incident management, information security aspects of business continuity management, and compliance; with internal requirements, such as policies, and with external requirements, such as laws

High redundancy, auto load balancing and scalable bandwidth on demand. eGOV Solutions Ltd monitor server performance and ensure high redundancy to deliver a fast service for users 24/7. Automatic load balancing enables 100% speed and scaleability of service guarantee for all clients on their dedicated servers. Typical load times for reports are 2 to 3 seconds

Scaleability of the eGOV platform has been designed and developed to fit mobile devices and smart devices. The service has also been developed as a direct APP with no differences to the service specification or requirements

Penetration testing every 6 months by 'IT Health Check' performed by a Tigerscheme qualified provider or a CREST-approved service provider

System usage and performance statistics, database reporting including self-service activity logs for user accountability, additional bespoke reports on request

ISSUE: Transfer of data between the school and the cloud
RISK: Risk of compromise and unlawful access when personal data is transferred.
MITIGATING ACTION: Encryption is identified in the UK GDPR as a protective measure that renders personal data unintelligible when it is affected by a breach

The browser utilises TLS 1.2 encrypted connections through a portal

ISO27001 certification demands best in class controls across: Information security policies, organisation of information security, human resource security, asset management, access control, cryptography, physical and environmental security, operations security, communications security, to comply such as laws

- **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: The ePEP infrastructure is built on AWS Cloud which provides multiple physically separated and isolated data centres providing high availability and highly redundant networking. Load balanced environment with scalable bandwidth on demand. All communications run inside ePEP VPN that is protected by a strict system of Firewall rules

  The data is stored in the AWS S3 storage service with high levels of durability and availability

ISO27001 certification demands best in class controls across: Information security policies, organisation of information security, human resource security, asset management, access control, cryptography, physical and environmental security, operations security, communications security, system acquisition, development and maintenance, supplier relationships, information security incident management, information security aspects of business continuity management, and compliance; with internal requirements, such as policies, and with external requirements, such as laws

- **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: Servers are UK based

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: ePEP Online administration control panel allows users to maintain and manage their own account CORE details including password resets and the ability to change their dual layer security question. Users can also access the ePEP support log and broadcast facility

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: All data is returned to the school by secure encrypted data transfer in a readable and useful format. On official request by the school eGov Solutions Ltd will hard delete all data and ensure this is destroyed in line with UK GDPR guidelines

  End of contract life exit will be discussed and agreed with the school to ensure that all statutory obligations are undertaken. Depending on the level of additional work and timeframe required there may be additional charges made to cover the technical involvement

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: eGOV Solutions Ltd systematically evaluate their information security risks, considering the impact of threats and vulnerabilities. Risks raised through

internal and external audits are reviewed at management meetings by their information security manager and head of business

eGOV Solutions Ltd design and implement a comprehensive suite of information security controls and other forms of risk management to address possible security risks to new and existing ePEP developments and services. eGOV Solutions Ltd continually review and update its security policies in line with ISO/IEC 27001:2013 security management standards

In the event of a data breach ePEP would notify users in keeping with the principles of data breach reporting as outlined by the ICO and ISO 27001

- **ISSUE:** Data is not backed up
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: External: all backup files are mirrored on a storage service with a different data centre in the UK to guarantee 99.9% uptime and secure storage disaster recovery.

  The backup system is managed in different ways: Hourly snapshots: copies of application servers and databases are automatically generated, creating a fast and secure restore point. The database failure system is fully automatic and does not require administrative intervention

  Individual: a backup script is scheduled hourly to generate an individual file for each client, allowing quick access to restore or analyse data without affecting the school

  ePEP can guarantee a network connectivity SLA level of 99.9 % uptime/availability results in the following periods of allowed downtime/unavailability: Daily: 1m 26s Weekly: 10m 4s Monthly: 43m 49s Yearly: 8h 45m 56s. This is to allow for service security updates and full data backups scheduled from 00.01 every day. This allows ePEP to guarantee 100% network connectivity and availability in normal day time and extended working hours. ePEP will refund the school one month's total costs if service is disrupted without a 3 minute response and resolution

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Servers are UK based

- **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: Under data protection law, data subjects have rights including: Right of access – Data subjects have the right to ask us for copies of your personal information. Right to rectification - Data subjects have the right to ask eGOV Solutions Ltd to rectify personal information they think is inaccurate. Data subjects also have the right to ask eGOV Solutions Ltd to complete information which they think is incomplete. Right to erasure - Data subjects have the right to ask eGOV Solutions Ltd to erase their personal information in certain circumstances. Right to restriction of processing - Data subjects have the right to ask eGOV Solutions Ltd to restrict the processing of their personal information in certain circumstances. Right to object to processing - Data subjects have the right to object to the processing of their personal information in certain circumstances. Right to data portability - Data subjects have the right to ask that eGOV Solutions Ltd transfer the personal information they gave us to another organisation, or to the data subject, in certain circumstances

  The Privacy Notice states that to exercise any of these rights, please contact DPO@cabinetoffice.gov.uk

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: eGov Solutions Ltd is the data processor, processing the school's personal data through the use of ePEP. The school as data controller still has ownership of the data

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

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: All users must authenticate and verify their individual email address and password. Once verified they need to complete specific characters from a memorable word at an ISO/IEC 27034 standard. Failed results will be blocked after 3 attempts and will be recorded/alerted to the client and the ePEP support team. The user would need to contact the national ePEP help number 24/7 to request and lift restrictions with additional verification

eGOV Solutions Ltd is ISO 27001 accredited and has Cyber Essentials

ISO 27001: is one of the most widely recognized, internationally accepted independent security standards. eGOV Solutions Ltd has earned ISO 27001 certification for the systems, applications, people, technology, processes, and data centres that make up its shared Common Infrastructure

This means that independent auditors have examined the controls protecting the data in eGOV Solutions Ltd systems (including logical security, privacy, and data centre security), and assured that these controls are in place and operating effectively

Cyber Essentials: Cyber Essentials is a government-backed certification scheme designed to protect organisations from 80% of common cyber-attacks and increase cyber security eGOV Solutions Ltd are certified with Cyber Essentials and are audited annually. This means eGOV Solutions Ltd IT systems are security approved by an accreditation body selected by the NCSC and eGOV Solutions Ltd have technical defences in place against cyber threats

eGOV Solutions Ltd has Business Continuity Management ISO 9001:2015

eGOV Solutions Ltd is registered with the Information Commissioner's Office (ICO) Registration Number: ZA513826

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 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 UK, Certified, Penetration Testing, Cyber essentials and ISO 27001	Reduced	Medium	Yes
Data Breaches	Documented in guidance from ICO and compliance with ISO 27001	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:		
DPO advice accepted or overruled by: Yes If overruled, you must explain your reasons		
Comments: DPO provided DPIA		
Consultation responses reviewed by: Retrospective – Platform imposed by LA 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