HALES VALLEY TRUST

Data Protection Impact Assessment (Provision Map)

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. **Priory Primary School** operates Provision Map which is a cloud based system. As such **Priory 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.

Priory Primary School recognises that moving to a cloud service provider has a number of implications. **Priory Primary School** recognises the need to have a good overview of its data information flow.

The Data Protection Impact Assessment looks at the wider context of privacy taking into account Data Protection Law and the Human Rights Act. It considers the need for a cloud based system and the impact it may have on individual privacy.

The school needs to know where the data is stored, how it can be transferred and what access possibilities the school has to its data. The location of the cloud is important to determine applicable law. The school will need to satisfy its responsibilities in determining whether the security measures the cloud provider has taken are sufficient, and that the rights of the data subject under the GDPR is satisfied by the school.

Priory Primary School aims to undertake this Data Protection Impact Assessment on an annual basis.

A Data Protection Impact Assessment will typically consist of the following key steps:

1. Identify the need for a DPIA.
2. Describe the information flow.
3. Identify data protection and related risks.
4. Identify data protection solutions to reduce or eliminate the risks.
5. Sign off the outcomes of the DPIA.

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
What is the aim of the project? – Provision Map is a management tool providing an 'at a glance' way of documenting and showing the range of provision, additional staffing and support that a school makes available to its pupils. Specifically it maps out SEN interventions helping professionals keep track with the pupil and staff involved in each intervention. It integrates SEN management cycle with automatic review reminders. Provision map generates cost, time, pupil premium and outcome reports in an instant. The outcome tracking feature makes it easier for the school to see the impact of the interventions and plans in place and for the school to take action accordingly. Pupil plans can also be shared with those that have parental responsibility. Edukey Education Ltd is the company supporting Provision Map. **Priory 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. Update of documents in real time 7. Good working practice, i.e. secure access to sensitive files Provision Map 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 and workforce) for the school provides the legitimate basis of why the school collects data. Provision Map is referenced in the respective Privacy Notices. The school acts as the data controller and Provision Map as the data processor. **How will you collect, use, store and delete data?** – The information collected by Provision Map is available on a secure online platform. 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. Provision Map collects personal data from the school's management information system which is RM Integris. **Will you be sharing data with anyone?** –**Priory 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, RM Integris and various third party Information Society Services applications. **Priory Primary School** agrees to maintain the security and integrity of the system by refraining from inappropriate sharing of data and maintaining system security at all times. **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.

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). Characteristics (such as ethnicity, language, nationality, gender, religion, data of birth, country of birth, free school meal eligibility). Special education needs, safeguarding information, medical and administration (doctors information, child health, dental health, allergies, medication and dietary requirements). Attendance information, assessment, attainment and behavioral information. The school also obtains data on parents/guardians/carers including their name, address, telephone number and e-mail address. Workforce data relates to personal information (such as name, address and contact details, employee or teacher number, salary, bank details, national insurance number, marital status, next of kin, dependents and emergency contacts). Special categories of data (such as gender, age, ethnic group). In particular, salary data is collected to enable the school to calculate the cost of interventions. **Special Category data?** – Some of the personal data collected falls under the GDPR special category data. This includes race; ethic origin; and health. **How much data is collected and used and how often?** – Provision Map software maps out interventions and keeps track of what pupils and staff are involved with. Where relevant personal data is collected for pupils within the school. This includes the pupil name, active learning plans, SEN support and parental comments against the pupil. **How long will you keep the data for?** – 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)? And what is the geographical area covered? Year 1 to Year 6 pupils **590** and workforce **84.**

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?** – **Priory Primary School** collects and processes personal data relating to its pupils to manage the parent/pupil relationship. Personal data is also collected for the workforce to assist reports, trends and profiling produced by Provision Map. Through the Privacy Notice (Pupil) and (Workforce) **Priory 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?** – 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?** – Some of the data may include special category data such as child safeguarding records, RM Integris, SEN records, Single Central Record. The cloud service provider may provide access controls to the files. For example, files designated as private – only you can access the files; public – everyone can view the files without any restriction; and shared – only people you invite can view the files. **Are there prior concerns over this type of processing or security flaws? –** All data is secured in transit using 256 bit SSL encryption. It is securely restored at rest within industry leading data storage standards. **Priory Primary School** recognises that moving to a cloud based solution raises a number of General Data Protection Regulations issues as follows: ▪ **ISSUE:** The cloud based solution will be storing personal data including sensitive information **RISK:** There is a risk of uncontrolled distribution of information to third parties. **MITIGATING ACTION:** Edukey Education Ltd school data is stored on approved and compliant cloud infrastructure. Access to all parts of the infrastructure is

available to Edukey Education Ltd staff on a need to know basis and access is always revoked as soon as a member of staff no longer needs access or leaves the company.

Security-centred code reviews and testing is performed on all newly developed features.
Regular vulnerability scanning is performed using in-house and independent (supplied by Detectify) automated vulnerability scanners.

Security related updates for all software used across the infrastructure is installed in a timely manner. Dual factor authentication is enforced for all Edukey staff and for all services used in relation to the product.

- **ISSUE**: Transfer of data between the school and the cloud
  RISK: Risk of compromise and unlawful access when personal data is transferred.
  MITIGATING ACTION: All data is secured in transit using 256 bit SSL whilst being transmitted over public and private networks. All data at rest is encrypted with AES256 block-based encryption.

- **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage.
  MITIGATING ACTION: Edukey Education Ltd's servers are hosted by Google Cloud and Rackspace in London, UK. The data centre is staffed by a team of highly trained, on-site engineers and security experts who work around the clock to ensure that the systems are secure and running strong. Data centres have built in multiple layers of redundancy, at every level - including physical security, power, cooling and networks. These redundancies help make the data centre more resilient and reliable.

  Physical security: Rackspace is restricted by biometric authentication, keycards and 24 x 7 x 365 surveillance. These ensure that only authorised engineers have access to routers, switches and servers. Google Cloud data centres incorporate multiple layers of physical security protections. Access to these data centres is limited to only a very small fraction of Google employees. They use multiple physical security layers to protect our data centre floors and use technologies like biometric identification, metal detection, cameras, vehicle barriers, and laser-based intrusion detection systems.

  Edukey Education Ltd back-up nightly and retain the last fourteen back-ups. Backups are managed by data centres and are redundant. They are in the same physical location (London) but on completely different servers.

- **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: Edukey Education Ltd servers are hosted by Google Cloud and Rackspace in the UK to ensure school data is retained within the European Economic Area.

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: GDPR non-compliance
  MITIGATING ACTION: Where it is necessary to access school data only approved Edukey Education Ltd support technical staff can access it. Edukey Education Ltd staff are vetted and are subject to contractual data access policies and confidentiality clauses. DBS checking is carried out on all staff.

  User access is based on individual usernames and passwords. User passwords must be a minimum of eight characters long and contain at least one number and one capital letter. Users have eight log-in attempts before they are locked out. Additional levels of security can be added such as locking access to the school IP address so that users need to be on site to gain access. Edukey Education Ltd commits to restrict access to customer data only to those individuals who require such access to perform their job function.

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: GDPR non-compliance
  MITIGATING ACTION: Edukey Education Ltd will delete all data 30 days after closing the school's account. The data will be completely eradicated fourteen days later from the company's backups. If a school cancels their contract with Edukey Education Ltd then their account is set into 'Awaiting Deletion' state. Deletion then occurs automatically within 30 days. Data remains in encrypted backups until the 30-day cycle is complete. All deletion of data and deletion of backup files are logged.

  Edukey Education Ltd can either provide, or will provide, means for authorised client users to implement data retention activities directly.

- **ISSUE:** Responding to a data breach
  RISK: GDPR non-compliance
  MITIGATING ACTION: In the first instance schools should contact their dedicated Edukey Education Ltd account administrator for any security issues, serious or minor. Edukey Education Ltd are committed to offering a transparent service whereby any customer who feels that he/she is not being dealt with appropriately can speak directly to the Director and/or Business Manager if they wish to. Telephone, email and remote support is instantly available. In the event of a serious incident, schools will have the full support of the company's technical team as a matter of priority until the issue is resolved.

- **ISSUE:** No deal Brexit
  RISK: GDPR non-compliance
  MITIGATING ACTION: Provision Map servers are hosted in the UK.

- **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: Provision Map has the capability to provide the schools with access to the data stored within. Where Subject Access Requests are made for specific areas of school data Edukey Education Ltd can either provide, or will provide, means for authorised client users to carry out activities directly

- **ISSUE:** Data Ownership
  RISK: GDPR non-compliance
  MITIGATING ACTION: The material generated by the school remains the property of the school.

- **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: Edukey Education Ltd use multiple protective layers with the cloud platform to protect its services. These include encryption and firewalling. The company carry out routinely vulnerability and penetration testing and promptly address any issues identified. This should be monitored to address any changes in technology and its impact on data. The school should maintain ownership of the Cloud technologies used ensuring the current and future technologies enable GDPR compliance

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

- **ISSUE:** Security of Privacy
  RISK: GDPR non-compliance
  MITIGATING ACTION: Edukey Education Ltd hold Cyber Essentials Certification - Certificate Number: IASME-A-07641. ICO registration number Z1932768. Google Cloud and Rackspace data centres are certified to the international standard for information security, ISO27001

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) ▪ Keeping Children Safe in Education 2018 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, Certified, Penetration Testing and Audit	Reduced	Medium	Yes
Data Breaches	Documented in contract and owned by school	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:	**Chief Executive Officer**	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	**Chief Executive Officer**	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 Provision Map 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?)* What is the cloud based solution chosen where data processing/storage premises are shared? *(Data is stored within an environment which utilizes state of the art network security, electronic surveillance, physical security and multi factor access control systems along to protect client data?)* *(2)* 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)* (3) What certification does Provision Map have?, *(e.g. ISO 27001 certified, registered with ICO, etc)*		
DPO advice accepted or overruled by:	**Yes**	If overruled, you must explain your reasons
Comments: **[DPO Advice provided]**		
Consultation responses reviewed by:	**Chief Executive Officer**	If your decision departs from individuals' views, you must explain your reasons

Comments:		
This DPIA will kept under review by:	**Your IG**	The DPO should also review ongoing compliance with DPIA