Data Protection Impact Assessment

(Early Years Provider Portal)

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/nursery. Hurst Green Primary School operates a cloud based system. As such Hurst Green 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.

Hurst Green Primary School recognises that moving to a cloud service provider has a number of implications. Hurst Green 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/nursery needs to know where the data is stored, how it can be transferred and what access possibilities the school/nursery has to its data. The location of the cloud is important to determine applicable law. The school/nursery 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/nursery.

Hurst Green Primary School aims to undertake this Data Protection Impact Assessment on an annual basis. A Data Protection Impact Assessment will typically consist of the following key steps:

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

5. Sign off the outcomes of the DPIA.

Contents

Step 1: Identify the need for a DPIA....3

Step 2: Describe the processing 5

Step 3: Consultation process 13

Step 4: Assess necessity and proportionality.... 13

Step 5: Identify and assess risks.... 15

Step 6: Identify measures to reduce risk 16

Step 7: Sign off and record outcomes.... 17

Step 1: Identify the need for a DPIA

Explain broadly what the 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? – Managing school/nursery child data is complex and time-consuming for local authorities, schools/nurseries and parents.

The school/nursery uses the Early Years Provider Portal which is part of the Synergy/Access Group to securely submit a child's attendance information to the Local Authority. The Early Years Provider Portal is used for a number of reasons by all OFSTED registered nurseries, childminders and schools/nurseries in Dudley to securely transfer data from the early year providers to the Local Authority. It's been in use since 2012, and over the years has grown in use to enable the secure transfer of Early Years Census data and child attendance data.

The use of the Early Years Provider Portal will help the school/nursery to deliver a cost-effective solution to meet the needs of the business.

Hurst Green 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/nursery 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/nursery 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/nursery's data unless they have been instructed by the school/nursery. The school/nursery's 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/nursery provides the lawful basis of why the school/nursery 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/nursery has considered the lawful basis by which it processes personal data. This is recorded in Hurst Green Primary 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/nursery is retained on the school/nursery's computer systems and in paper files. The information is also stored on a hosted server at Dudley MBC. The information is retained according to the school/nursery's Data Retention Policy.

What is the source of the data? – Pupil information is collected via registration forms when pupils join the school/nursery, pupil update forms the school/nursery issue at the start of the year, Common Transfer File (CTF) or secure file transfer from previous schools/nurseries. Pupil information also includes classroom work, assessments and reports.

Will you be sharing data with anyone? – Hurst Green Primary School routinely shares pupil information with relevant staff within the school/nursery, school/nursery that the pupil attends after leaving, the Local Authority, the Department for Education, Health Services, Learning Support Services, schools/nursery 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/nursery to the Dudley MBC server. Storage of personal and 'special category data in the Cloud. However, in terms of using the Early Years Provider Portal the use of special category data will be limited to the lawful basis as outlined in the school/nursery 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 (siblings, siblings gender, siblings date of birth), Court Order, Education Health Care Plan (EHCP), Looked After Child (LAC)). School/nursery Preference and reasons for school/nursery choice and distance from home to school/nursery. The school/nursery also obtains data on parents/guardians/carers including their name, address, telephone number and e-mail address.

Special Category data? – Some of the personal data collected falls under the UK GDPR special category data. This includes health. In terms of using Early Years Provider Portal:

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/nursery will ensure that it has a lawful basis to do this and that this is documented in the school/nursery'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/nursery 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?

Early Years Provider Portal will be used by the school/nursery to manage the secure transfer of school/nursery attendance information to the Local Authority.

The school/nursery will act in accordance with the lawful basis it has for using personal data. This is outlined in the school/nursery's 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/nursery provides education to its students with staff delivering the National Curriculum.

What is the nature of your relationship with the individuals? – Hurst Green Primary School collects and processes personal data relating to its pupils to manage the school/nursery and parent/pupil relationship.

Through the Privacy Notice (Pupil) Hurst Green 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. Dudley MBC is hosting the data and will not be accessing it. The school/nursery 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/nursery may have.

Do they include children or other vulnerable groups? – In terms of the Early Years Provider Portal special category data may be collected to assist in the funding process.

Whatever special category data is used the school/nursery will ensure that it has a lawful basis to do this and that this is documented in the school/nursery'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 since the encryption key will need to be shared with others to access the data.

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

- **ISSUE:** Dudley MBC will be storing personal data including sensitive information
  RISK: There is a risk of uncontrolled distribution of information to third parties.
  MITIGATING ACTION: The Synergy servers are all stored in the Dudley Council Data Centres, which have secure physical access controls to them. The servers are maintained by Dudley's ICT Infrastructure staff and have all the necessary security patches installed whenever they are released by Microsoft.

  Whenever there is a new version of the Synergy software released and upgraded to the Synergy servers, a 3rd party cyber security service provider is contracted to perform the necessary vulnerability and penetration testing.

ISSUE: Transfer of data between the school/nursery 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 school/nursery pupil data is stored in a SQL server database that uses Transparent data encryption (TDE) encryption.

The Early Years and Childcare Strategy Team have access to the data, along with the ICT Application Support Team staff. Controls are in place to only allow staff access to the Synergy system who have been authorised to do so

All external traffic is secured with a TLS certificate using TLS 1.2 encrypted connections through a portal.

- **ISSUE:** Use of third party sub processors?
  RISK: Non compliance with the requirements under UK GDPR
  MITIGATING ACTION: No, the data is only used by local Dudley schools, nurseries or childminders

- **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: The Synergy servers are all stored in the Dudley Council Data Centres, which have secured physical access controls for them. The servers are maintained by Dudley's ICT Infrastructure staff and have all the necessary security patches installed whenever they are released by Microsoft.

  The Synergy servers are installed in the virtual "server farm", so if more disc space or extra processing resources are needed, a Dudley ICT engineer can allocate more resource to the Synergy 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: 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: When operating as a processor, Dudley MBC makes available to schools and nurseries as data controllers, the personal data of its data subjects and the ability to fulfill any data subject access requests when data subjects exercise their rights under the UK GDPR. This is done in a manner consistent with the functionality of the Early Years Provider Portal.

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The school/nursery will implement its data retention as appropriate and in accord with the school/nursery's data retention policy.

  This is in keeping with the principle of Article 5 1 e personal data shall be 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed' (the principle of 'storage limitation').

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Dudley MBC is committed to helping protect the security of the school/nursery's information. In compliance with the provisions of Article 32 of the UK GDPR, Dudley MBC has implemented and will maintain and follow appropriate technical and organizational measures intended to protect school and nursery data against accidental, unauthorized, or unlawful access, disclosure, alteration, loss, or destruction.

  Suspected breaches are notified to the Early Years and Childcare Strategy Team Manager, and would be logged, which then goes to the Corporate Information Governance Team for investigation.

  Dudley MBC will work with the school/nursery to resolve any data breaches.

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

MITIGATING ACTION: The Synergy servers are mirrored across the 2 Dudley data centres. Backups are performed every night and using 'mirrored' servers means no data would be lost.

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

- **ISSUE:** Subject Access Requests
  RISK: The school/nursery 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 Early Years Provider Portal to rectify personal information they think is inaccurate. Data subjects also have the right to complete information which they think is incomplete. Right to erasure - Data subjects have the right to erase their personal information in certain circumstances. Right to restriction of processing - Data subjects have the right 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 transfer the personal information they gave us to another organisation, or to the data subject, in certain circumstances.

  School/nurseries will provide all the necessary information support any requests made by the data subject(s).

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Synergy/Access Group is the data processor, processing the school's personal data through the use of the Early Years Provider Portal. The school/nursery 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 Early Years Provider Portal.

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  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 school/nursery pupil data is stored in a SQL server database, so it uses Transparent data encryption (TDE) encryption.

  The Early Years and Childcare Strategy Team have access to the data, along with the ICT Application Support Team staff. Controls are in place to only allow staff access to the Synergy system who have been authorised to do so.

  All external traffic is secured with a TLS certificate using TLS 1.2 encrypted connections through a portal.

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/nursery 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/nursery has a Subject Access Request procedure in place to ensure compliance with Data Protection Law

The cloud based solution will enable the school/nursery 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/nursery 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	Reduced	Medium	Yes
Data Breaches	Documented in Synergy/Access Group Services Terms	Reduced	Low	Yes
Subject Access Request	Technical capability to satisfy data subject access request	Reduced	Low	Yes
Data Retention	Implementing school/nursery data retention periods in the cloud	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Headteacher	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	DPO	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:

Clarification has been sort on the following from Synergy/Access Group's DPO. The answers have been incorporated in the risk, issues and mitigation log in section 2 of this DPIA:

1. What is the 'upload' process? If through a website portal, how is the data secured in transit between the school/nursery and Dudley MBC servers? ie. Does the browser utilise TLS/SSL connections with AES-256bit encryption?
2. Could you please advise what server hosting services and the physical access controls, security of the servers, permission-based access, CCTV recording, Cyber Essentials certification, vulnerability and penetration testing?
3. Is any data transferred or shared with partners or third parties outside of the UK?
4. Should demand unexpectedly increase, can the Dudley MBC server hosting the Early Years Provider Portal service scale their facilities to meet demand?
5. What resiliency does the Dudley MBC server hosting service provide for the availability of data? E.g. mirrored data centres, how often are backups taken and how long would it take to restore from an outage? Does the service manage all security updates for the service?
6. Is school/nursery data encrypted at rest on the hosting servers? Who has access to the data and what access controls do you put into place?
7. What is the data breach notification process?
8. Clarification on data retention period?

DPO advice accepted or overruled by:

Accepted

If overruled, you must explain your reasons

Comments:		
Consultation responses reviewed by: Headtaecher If your decision departs from individuals' views, you must explain your reasons		
Comments:		
This DPIA will kept under review by:	School Business Manager	The DPO should also review ongoing compliance with DPIA