Data Protection Impact Assessment (SchoolGrid)

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. Hurst Green Primary School operates a cloud based system called SchoolGrid. 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 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. 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

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? – SchoolGrid offers a fully integrated software solution via a Portal to facilitate contact free ordering and payment for school meals which is designed to help schools reduce the time taken to administer expenditure every day.

The software is installed locally on a PC which links to a hosted database. SchoolGrid keeps track of individual pupil's balances as meals are recorded and payments taken, including the option for parents to order and pay meals online. SchoolGrid can be accessed through the Portal by the user via mobile devices.

SchoolGrid has the following functionality:

- *Pre-ordering & parent payments (cards)* –SchoolGrid manages card payments. Any cash can be accommodated by the system. Pupil account histories are automatically stored, enabling auditing

- *Menu planning, recipes, nutrition & allergy protection* – SchoolGrid makes selection and delivery easy with a pupil personalised dietary requirement inbuilt into the system

- *Parent communication and feedback tools* – SchoolGrid collect dish star ratings, run on-screen micro surveys and provide a parent compliments system.

- *Advanced Reporting* – SchoolGrid provides a range of useful reports which help schools keep track of meal numbers, payments and banking. This gives a school insight on pre-orders and uptake, and export information easily for auditing purposes.

Personal data is collected through a number of channels dependent on the schools implementation of the solution. Student data and the associated data fields can be captured through a manual upload. Parent's sign a consent form and admin staff manually upload the parent and child details onto schoolgrid. Personal data is not pulled through any other system in school, there is no link with Wonde or MIS.

School payment system parent data and the associated data fields can be captured through self registration online.

SchoolGrid links to the school's management information system which ensures pupils records are kept up to date. Pupil data is uploaded into the Portal using the school's management information system. The school can record free school meals.

Wonde and Third Party Apps/Vendors

Wonde's core service is used by a large percentage of schools in the UK to control the Management Information System (MIS) data it shares with third party vendors used at the school. These vendors include solutions for assessment, maths, English, library management, parent communications, parent payments, Multi Academy Trusts, voucher systems, Google/Microsoft syncing, classroom content providers etc.

Wonde is ISO27001 accredited and the majority of schools use Wonde to manage their MIS data sharing and syncing with multiple third party vendors.

When a vendor (app), or vendors, requests to be connected to a school via Wonde - if the school approves that vendor(s) request and for Wonde to facilitate it, then Wonde will complete a base integration with the schools' MIS. Wonde request (but do not extract) the permissions that are required for the majority of vendors that use its services. Wonde will then only extract and send data that has been approved by a school to send onwards to their chosen vendors. For clarity, Wonde does not extract data that is not approved by the schools for the vendors they are using.

Hurst Green Primary School can reduce the requested Wonde permissions upon the integration taking place, and Wonde can assist schools with this. Hurst Green Primary School also has the ability to change the permissions whenever it likes, but in doing so ensures that it has considered how that may affect its use of approved vendors (i.e. the flow of data to those vendors via Wonde for the vendors to provide the agreed service).

[school to delete this Wonde and Third Party Apps/Vendors section if not appropriate]

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 aims to achieve the following:

1. Scaleability
2. Reliability
3. Resilience
4. Delivery at a potentially lower cost
5. Supports mobile access to data securely
6. Good working practice

SchoolGrid will enable the user to access information via the Portal from any location or any type of device (laptop, mobile phone, tablet, etc).

The cloud service provider cannot do anything with the school's data unless they have been instructed by the school. The schools Privacy Notice will be updated especially with reference to the storing of pupil in the cloud.

Step 2: Describe the processing

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

The Privacy Notices (pupil) for the school provides the 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 highlighted consent as the lawful basis by which it processes personal data. This is recorded in Hurst Green Primary School Privacy Notice (Pupil).

How will you collect, use, store and delete data? – The information collected by the school is retained on the school's management information system. SchoolGrid obtains personal data from the school's management information system. This includes the pupil name, date of birth, pupil year group, dietary preferences, food allergies, account balance and free school meals. This also includes details of parental responsibilities and their

contact details including parent name, parent e-mail, telephone number and address. The information is retained according to the school's Data Retention Policy.

What is the source of the data? – Pupil information is collected via registration forms when pupils join the school, pupil update forms the school issue at the start of the year, Common Transfer File (CTF) or secure file transfer from previous schools.

Will you be sharing data with anyone? – Hurst Green 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.

Within the context of SchoolGrid it manages the payment processing of the transaction.

What types of processing identified as likely high risk are involved? – Transferring personal data from the school to the cloud. Storage of personal data in the Cloud. SchoolGrid has the potential for collecting biometric information through the mapping of a students face or finger print. It also will collect information medical dietary requirements. Where biometric data is used consent will have been obtained by the school.

[school to delete information relating to biometric data if not appropriate in the local setting]

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

What is the nature of the data? – Pupil data relates to personal identifiers and contacts (such as name, unique pupil number, contact details and address). The Privacy Policy for SchoolGrid states that the following personal data will be collected: name of parent or guardian, email address, phone number, details of pupils school and year group, free schools meals and transaction history. Where applicable this will also include biometric medical data.

[school to delete information relating to biometric data if not appropriate in the local setting]

The information is sourced from Hurst Green Primary School the management information system.

Special Category data? – SchoolGrid has the potential for collecting biometric information through the mapping of a students face or finger print. It also will collect information medical dietary requirements. Where biometric data is used consent will have been obtained by the school.

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.*

[school to delete information relating to biometric data if not appropriate in the local setting]

How much data is collected and used and how often? – Personal data is collected for all pupils and their respective parent/guardians. Additionally personal data is also held respecting school administrative contact details, school name and address, school e-mail address, school contact telephone number, and staff information (staff name, staff e-mail address, staff teaching groups).

How long will you keep the data for? – The school will consider the data retention period as outlined in the IRMS Information Management Toolkit for Schools.

Scope of data obtained? – How many individuals are affected (pupils, workforce, governors, volunteers)? And what is the geographical area covered? Reception and [Year X] to [Year X] pupils [pupil roll], and workforce [insert number].

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? – **Hurst Green Primary School** collects and processes personal data relating to its pupils and employees to manage the parent/pupil and employment relationship.

Through the Privacy Notice (pupil/workforce) 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? – SchoolGrid users (parents, staff) may have individual user accounts to log into the Portal to retrieve information.

Do they include children or other vulnerable groups? – Yes. Some of the data used may be classified under UK GDPR as special category. Additionally, personal data will be collected: pupil information including the pupil name, pupil UPN (unique pupil number), pupil class name, and details of those that have free school meals.

Are there prior concerns over this type of processing or security flaws? – SchoolGrid implement appropriate technical and organizational measures to protect Personal data against accidental or unlawful alteration or loss, or from unauthorized, use, disclosure or access, in accordance with their Group Information & Systems Security Policy. This includes personal data is encrypted in transit and at rest. Annual penetration test is conducted on the system and remediated where required. Weekly vulnerability scans are conducted on the system and remediated where required.

Hurst Green Primary School has the responsibility to consider the level and type of access each user will have.

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

- **ISSUE:** The management information system will be storing biometric data 'special category' information
  RISK: There is a risk of obtaining biometric data for other purposes
  MITIGATING ACTION: Biometric data is stored securely and encrypted in transit and at rest. Annual penetration test is conducted on the system and remediated where

required. Weekly vulnerability scans are conducted on the system and remediated where required

[school to delete information relating to biometric data if not appropriate in the local setting]

- **ISSUE:** The cloud based solution will be storing personal data
  RISK: There is a risk of uncontrolled distribution of information to third parties
  MITIGATING ACTION: Access is via web browser. User accounts are role-based and roles will determine access to features/functions of the system. Users login using a password and SchoolGrid enforce a minimum 12 character password length and 6 month password expiry. SchoolGrid also do support MFA

  SchoolGrid implement appropriate technical and organizational measures to protect Personal data against accidental or unlawful alteration or loss, or from unauthorized, use, disclosure or access, in accordance with their policies. This includes personal data is encrypted in transit and at rest. Annual penetration test is conducted on the system and remediated where required. Weekly vulnerability scans are conducted on the system and remediated where required

- **ISSUE**: Transfer of data between the school and the cloud
  RISK: Risk of compromise and unlawful access when personal data is transferred
  MITIGATING ACTION: SchoolGrid are aware that the transmission of information via the internet is not completely secure. Although they will do their best to protect personal data, they cannot guarantee the security of data transmitted to the Application; any transmission is at the school's own risk. Once SchoolGrid have received the school's information, it will use strict procedures and security features to try to prevent unauthorised access. This includes personal data is encrypted in transit and at rest. Annual penetration test is conducted on the system and remediated where required. Weekly vulnerability scans are conducted on the system and remediated where required

- **ISSUE:** Use of third-party sub processors?
  RISK: Non-compliance with the requirements under UK GDPR
  MITIGATING ACTION: SchoolGrid will not disclose personal data to any unauthorized third parties. Personal data will only be available to internal or external third parties, who need such access or where required by law, for claims or to prevent fraud. Personal

data may be shared only where necessary, for fulfilment of an order, where joint services are provided, or for legal, reporting or business re-organisation

Where SchoolGrid utilise a handful of sub-processors they are all UK/EU based.

- **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: All data is hosted within the UK/EU and does not leave that boundary

  Where SchoolGrid do store data outside the EEA, it will take all reasonable steps to ensure that school data is treated as safely and securely as it would be within the UK and under the Data Protection Act 2018, and the GDPR including: Requiring services to meet ISO 27001 Security Management Standards and requiring services to have Independent security testing and verification

- **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: Personal data will be stored in the UK

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: SchoolGrid's Privacy Notice states it is committed to ensure protection of data subject rights under applicable laws. These rights are summarised in the privacy notice

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Depending on the school's use of the site, and use of the provided payment options (such as DIrect Debit) SchoolGrid may be legally required to keep some school details for up to 6 years, or indefinitely (as is the case with Direct Debit user data). Where this is not legally required, SchoolGrid will remove data 12

calendar months following deactivation of pupil and parent accounts by the school office

- **ISSUE:** Data Back ups
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: SchoolGrid employ various strategies for reliability and resilience. SchoolGrid regularly backup our database and retain 7 days of backups and then 3 months of weekly backups followed by monthly backups thereafter. From an application perspective, SchoolGrid utilise premium tier Azure resources as recommended for production workloads as well as load balancing. SchoolGrid would expect to restore service within 4 hours depending on the nature of the outage

  SchoolGrid Micosoft Azure. Data is backed up in accordance with Azure SQL backup and retention policy: https://docs.microsoft.com/en-us/azure/azure-sql/database/automated-backups-overview?tabs=single-database

  Both SQL Database and SQL Managed Instance use SQL Server technology to create full backups every week, differential backups every 12-24 hours, and transaction log backups every 5 to 10 minutes. The frequency of transaction log backups is based on the compute size and the amount of database activity

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: SchoolGrid have a data breach policy which follows a framework of investigation and assessment -> containment and recovery -> notification -> review. During the notification process SchoolGrid will ensure all relevant stakeholders are made aware of the issue and the remedial actions

  SchoolGrid have a formalised incident response plan documented internally that is tested and reviewed on at least an annual basis

- **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: SchoolGrid Privacy Notice states that data subjects have the right to ask for a copy of any of their personal data held by SchoolGrid (where such data

is held). Under the GDPR, no fee is payable and SchoolGrid will provide any and all information in response to a request free of charge. Subject Access Request enquries should be directed to dataprotection@schoolgrid.co.uk

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: SchoolGrid does not share or disclose any of the school's personal information without the school's consent. SchoolGrid is acting as a data processor and the ownership of the personal data remains with 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: This should be monitored to address any changes in technology and its impact on data to enable UK GDPR compliance

- **ISSUE:** UK GDPR Training
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: SchoolGrid staff receive role-focused training and are only given system access if relevant to their role. Appropriate training is therefore undertaken by personnel that have access to the SchoolGrid Portal

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Personal information used in the SchoolGrid platform is always kept to a minimum and is only visible by staff elected by the school. SchoolGrid will not access this information unless it is deemed necessary to do so for the purposes of support and in any instance will only access this information with permission from the school. SchoolGrid implement user authentication when accessing personal data

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

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

The school moving to a cloud based solution will realise the following benefits:

1. Scaleability
2. Reliability
3. Resilience
4. Delivery at a potentially lower cost
5. Supports mobile access to data securely
6. Good working practice

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

The views of senior leadership team and the Board of Governors will be obtained. Once reviewed the views of stakeholders will be taken into account. The view of YourIG has also been engaged to ensure Data Protection Law compliance

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

The lawful basis for processing personal data is contained in the school's Privacy Notice (Pupil and Workforce). The lawful 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 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

16

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. Encrypted in transit and at rest	Reduced	Medium	Yes
Data Breaches	SchoolGrid ability to respond and deal with a data breach	Reduced	Low	Yes
Subject Access Request	Technical capability to satisfy data subject access request	Reduced	Low	Yes
Data Retention	Implementing school data retention periods in the cloud	Reduced	Low	Yes

17

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:	Headteacher	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) How is access to the platform managed e.g. through the web browser? Does it offer individual user accounts with role-based permissions? Is access granted through passwords, or is MFA offered?
(2) Does the platform utilise Wonde for the secure transfer of data between the school's MIS and SchoolGrid and then again between the platform to the receiving school?
(3) ISO27001 is mentioned on your website, could you confirm which cloud platform you are using to host the data (eg. MS Azure, Amazon AWS)?
(4) Does the platform utilise the latest TLS / SSL encryption methods to transfer data (eg. TLS 1.2 / 128 or 256-bit AES)?
(5) Is the data encrypted at rest?
(6) Should there be an outage within the data centre, how quickly can service be restored and what sort of resiliency does the platform have (eg. backups, retained for xx days, mirrored servers)?
(7) Should demand unexpectedly increase, can your server hosting service scale their facilities to meet demand?
(8) Other than the hosting company, does SchoolGird utilise other third-party processors? Eg. for managing direct debits, offering support and if so where are these sub-processors located?
(9) Confirmation that all data is hosted within the UK/EU and no personal data is transferred outside this area?
(10) What training is provided to SchoolGrid staff, do they have DBS clearance and what access to the customer data do they have?
(11) If there is a suspected data breach, how will the SchoolGrid team work with the school?

DPO advice accepted or overruled by: YES Accepted If overrule you must explain your reasons		
Comments: YourIGDPO Service liaised with supplier for further clarification as outlined above in summary of DPO advice. The responses have been incorporates into section 2		
Consultation responses reviewed by: Headteacher If your decision departs from individuals' views, you must explain your reasons		
Comments: None		
This DPIA will kept under review by:	School Business Manager	The DPO should also review ongoing compliance with DPIA