Data Protection Impact Assessment(Dolce Catering)

Hurst Green Primary School uses Dolce Catering to provide its school meals service. It provides a variety of menus which vary in Spring, Summer and Autumn. To provide an online pre-order and payment system Dolce Catering uses SchoolGrid. SchoolGrid enables parents to place orders online using Dolce Catering's online app. 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 new 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? –Dolce Catering provides a fully managed catering service to Hurst Green Primary School. In doing so it will help deliver a cost effective and value for money service to meet the needs of the school.

Dolce Catering provides an integrated software solution designed to help schools reduce the time taken to administer expenditure every day. The software is hosted in the cloud via Microsoft Azure Services. The software is provided via web access. Dolce Catering via 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.

Dolce Catering provides an audit trail of payments and expenditure. As payments are received these are added against the pupil's record. Receipts can be issued and bespoke reports produced; i.e. relating to school dinners to manage outstanding balances.

It enables a school to set up and select their own lunch options, along with prices. Once the meals are recorded the school can generate a report to let the kitchen know how many meals to prepare. It also enables Hurst Green Primary School in the management of allergens and how they can ensure no child receives an ingredient they are allergic too.

Dolce Catering can link to the school's management information system which ensures pupils records are kept up to date. Pupil data is uploaded into Dolce Catering using either csv file generated from the school's management information system or directly from the school's management information system. The school can record free school meals.

SchoolGrid is a secure online payment system used by Dolce Catering.

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 Dolce Catering 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

Dolce Catering will enable the user (parent or guardian) to access information from any location or any type of device via its online app.

Dolce Catering 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 personal data used, where it is stored and the retention period.

SchoolGrid is a data processor that provides services on behalf of the caterer and school where meals are provided.

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 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. Dolce Catering obtains personal data from the school’s management information system and/or via csv file. This includes the pupil name (first and last name), date of birth, unique pupil number, management information system ID, academic year, allergens, and free school meal entitlement. This also includes details of parental responsibilities and their contact details. 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.

SchoolGrid obtains direct debit or credit card information from the parent/guardian to support payment options. Linked to Dolce Catering it enables parents/guardians to control their child's school meal service, providing nutrition and allergy information to parents/guardians, contacting parents/guardians possibly in the case of an emergency, and providing parents/guardians with cashless payment options.

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 Dolce Catering there is an interface with SchoolGrid. Personal data is only used by SchoolGrid for legal reasons, food ordering and dietary requirements purposes. UK GDPR prohibits SchoolGrid sharing personal data with third parties accept with express permission of the individual. There is no sharing of data outside of SchoolGrid unless permission has been sufficiently granted.

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.

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 Dolce Catering states that the following personal data will be collected: pupil information including the pupil name, pupil UPN (unique pupil number), pupil class name, and details of those pupils that have free school meals.

As SchoolGrid allows for pre order by parents contact details such as e-mail address and parent name may also be required from the school's management information system.

SchoolGrid obtains parental/guardian information relating to direct debit or credit card information to support payment options.

Data may also be provided directly to SchoolGrid from the pupil's school. This may include pupil information, parent/guardian name, and parent/guardian e-mail address.

The information is sourced from Hurst Green Primary School either the management information system or imported manually import csv file format.

Special Category data? – None of the data is classified under UK GDPR as special category.

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 and Schools Data Retention Policy.

Scope of data obtained? – How many individuals are affected (pupils, workforce, governors, volunteers)? And what is the geographical area covered? Reception and Year 1 to Year 6 pupils 420, and workforce 60.

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? – Dolce Catering users (parents, staff) may have individual user accounts to log into SchoolGrid to retrieve information.

Do they include children or other vulnerable groups? – None of the data is classified under UK GDPR as special category. However, 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? – Data is received by API end points hosted in SchoolGrid's Secure Data Centre, this data is encrypted in transit using TLS 1.2, and subsequently stored at rest within an encrypted database.

SchoolGrid performs routine backups and tests that those backup procedures are sufficient. Microsoft Azure Services allow for ease of service restoration. There Service Level Agreement states a commitment for a high availability policy.

In terms of application security, users (staff) can log into the SchoolGrid IOS and android mobile applications and view user specific data. SchoolGrid have a number of options to control the level of access to data for a user.

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 cloud based solution will be storing personal data
  RISK: There is a risk of uncontrolled distribution of information to third parties
  MITIGATING ACTION: All of our infrastructure is hosted by Microsoft Azure Services with geo redundancy, our site is accessed via authenticated users that have specific claims based access to data. All server instances are only accessible via a virtual private network which requires specific access grants assigned to individuals that require access. Encryption technology may be used to enhance information privacy and help prevent loss, misuse, or alteration of the information under the control of Dolce Catering/SchoolGrid. Servers are located in an ISO 27001 certified data centre within the UK. All of the servers are protected by physical firewalls

- **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 uses industry standard encryption practices (TLS 1.2). All data is encrypted at rest. Access to the servers is protected by a virtual network gateway

- **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: SchoolGrid holds ISO 27001, ISO 18001 and ISO 9001

- **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: SchoolGrid do not share personal data outside of the EEA (see exception comment in No Deal Brexit)

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Dolce Catering are developing an Individuals Rights Policy

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The personal data will be managed in line with the school's data retention policy. Personal data is retained as long as it is legally necessary for SchoolGrid. Once determined there is no legal need to retain said data, that data will be removed from the system within a twelve month period

- **ISSUE:** Data Back ups
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: SchoolGrid performs routine backups and tests that those backup procedures are sufficient. Microsoft Azure Services allow for ease of service restoration. There Service Level Agreement states a commitment for a high availability policy

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance

  MITIGATING ACTION: Dolce Catering are developing a Data Breach Policy

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: SchoolGrid is hosted within the UK. School Grid uses Google for its e-mail and document editing systems where personal data is transferred to the USA. School Grid use Privacy Shield to ensure UK GDPR compliance

  The European Court of Justice (ECJ) has ruled that the EU-US Privacy Shield is invalid as it fails to protect privacy and data protection rules. As part of the same ruling the ECJ decided that another data transfer mechanism, Standards Contractual Clauses, or SCCs, remain valid. The school will need to confirm whether an SCC is in place

- **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: Dolce Catering are developing a Subject Access Requests Policy

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Dolce Catering/SchoolGrid does not share or disclose any of the school's personal information without the school's consent. Dolce Catering/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: Dolce Catering have reviewed their technology platforms and usage and will gain Cyber Essentials Certification as a further risk reduction strategy with ongoing testing timetabled to ensure Dolce Catering's layered defences are fully operational

- **ISSUE:** UK GDPR Training
  RISK: UK GDPR non-compliance

MITIGATING ACTION: Appropriate training is undertaken by personnel that have access to Dolce Catering

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Personal information used in the Dolce Catering/SchoolGrid platform is always kept to a minimum and is only visible by staff elected by the school. Dolce Catering/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. Dolce Catering/SchoolGrid implement user authentication when accessing personal data

  SchoolGrid holds ISO 27001, ISO 18001 and ISO 9001

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 Dolce Catering 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 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. Accredited to ISO 27001 and PCI Data Security Standard	Reduced	Medium	Yes
Data Breaches	Dolce Catering/School Grid 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

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) Is the software used by Dolce Catering downloaded locally (the school) with communication to servers held offsite? *The software is hosted in the cloud via Microsoft Azure Services, the software is provided via web access.*

(2) Is personal data shared electronically between Dolce Catering and SchoolGrid and vice versa? *The personal data is only used by SchoolGrid for legal, food ordering and dietary requirements purposes. GDPR prohibits SchoolGrid sharing personal data with third parties accept with express permission of the individual.*

(3) During set up does Dolce Catering take personal information from the school's management information system or csv? And if so what data does it use, i.e. name of pupil, UPN, free school meals, allergies, etc? *The initial data collected will be provided via a csv to import into the system. As SchoolGrid allows for pre order by parents some and email address and parent name may also be required. SchoolGrid requires pupil information (Forename, Surname, Date of Birth, Add No, MIS Id, Academic Year, Allergens, Free School Meal Entitlement.*

(4) YourIG's understanding is that the school is the data controller and Dolce Catering is the data processor? *SchoolGrid is a data processor that provides services on behalf of the caterer and school where meals are provided.*

(5) During transfer of personal data is end to end encryption used during transit? i.e. strong SHA-2/2048 bit encryption, etc. Is encryption used when personal data is at rest (Dolce Catering and SchoolGrid)? *SchoolGrid uses industry standard encryption practices (TLS 1.2) all data is encrypted at rest. Access to the servers is protected by a virtual network gateway.*

(6) What security procedures does Dolce Catering/School Grid have in place to restrict access to personal data, especially where the data is kept at the data centre? i.e. where are servers located, what are the certified security and regulations? Are the servers located behind firewalls? *All of our infrastructure is hosted by Microsoft Azure Services with geo redundancy, our site is accessed via authenticated users that have specific claims based access to data. All server instances are only accessible via a virtual private network which requires specific access grants assigned to individuals that require access.*

(7) Where applicable what are the contingency arrangements around a no deal Brexit? *SchoolGrid will maintain normal operations in the occurrence of a no deal Brexit.*

(8) Is any of the data shared outside of the EEA (Dolce Catering and SchoolGrid)? *There is no sharing of data outside of SchoolGrid unless permission has been sufficiently granted.*

(9) Dolce Catering have said that they are developing guidance on individuals rights, subject access requests and data breach guidance. Could the school have copies please? *Our privacy policy is located here:* https://cdn.schoolgrid.co.uk/termsofuse/Privacy-Policy.pdf

(10) How long in personal data retained by Dolce Catering and SchoolGrid? *Personal data is retained as long as it is legally necessary for SchoolGrid. Once determined there is no legal need to retain said data, that data will be removed from the system within a twelve month period.*

(11) Data backups and which services are used (Dolce Catering and SchoolGrid)? *SchoolGrid performs routine backups and test that those backup procedures are sufficient. Microsoft Azure Services allow for ease of service restoration where there SLA provides a high availability policy.*

(12) Does Dolce Catering and SchoolGrid have quality standards, ie. ISO 27001, etc? *SchoolGrid holds ISO 27001, ISO 18001, ISO 9001*

DPO advice accepted or overruled by: Yes If overruled, you must explain your reasons		
Comments: YourIGDPO Service liaised with supplier for further clarification as outlined above in summary of DPO advice.		
Consultation responses reviewed by: 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