Data Protection Impact Assessment (Relish School Food)

Cloud computing is a method for delivering information technology (IT) services in which resources are retrieved from the Internet through web-based tools and applications, as opposed to a direct connection to a server at the school. Old Park School operates a cloud based system called Relish School Food Ltd. As such Old Park School must consider the privacy implications of such a system. The Data Protection Impact Assessment is a systematic process for identifying and addressing privacy issues and considers the future consequences for privacy of a current or proposed action. Old Park School recognises that moving to a cloud service provider has a number of implications. Old Park School recognises the need to have a good overview of its data information flow. The Data Protection Impact Assessment looks at the wider context of privacy taking into account Data Protection Law and the Human Rights Act. It considers the need for a cloud based system and the impact it may have on individual privacy.

The school needs to know where the data is stored, how it can be transferred and what access possibilities the school has to its data. The location of the cloud is important to determine applicable law. The school will need to satisfy its responsibilities in determining whether the security measures the cloud provider has taken are sufficient, and that the rights of the data subject under the UK GDPR is satisfied by the school. Old Park School aims to undertake this Data Protection Impact Assessment on an annual basis.

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

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

Contents

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

What is the aim of the project? – Relish School Food Ltd offers a fully integrated software solution via the Relish app 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. Relish School Food Ltd 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. Relish School Food Ltd can be accessed through the Relish app by the user via mobile devices.

The Relish app 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 outstanding balances, etc.

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.

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 the following channels: - (1) Manual upload through back of house web application; (2) Automated upload through school MIS system; or (3) Automated upload through integrated 3rd party.

School payment system parent data and the associated data fields can be captured through the following channels: - (1) Self registration through online web solution; (2) Self registration through native mobile app solution or (3) Automated upload through school MIS system.

The Relish app links to the school's management information system which ensures pupils records are kept up to date. Pupil data is uploaded into the Relish app 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. An overview of how schools do this can be found here https://www.wonde.com/school-data-management.

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.

Old Park School can reduce the requested Wonde permissions upon the integration taking place, and Wonde can assist schools with this. Old Park 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).

Old Park School will undertake the following processes:

1. Collecting personal data
2. Recording and organizing personal data
3. Structuring and storing personal data
4. Copying personal data

5. Retrieving personal data
6. Deleting personal data

By opting for a cloud based solution the school aims to achieve the following:

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

Relish School Food Ltd will enable the user to access information via the Relish app 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 Old Park School Privacy Notice (Pupil) and (Workforce).

How will you collect, use, store and delete data? – The information collected by the school is retained on the school's management information system. Relish School Food Ltd obtains personal data from the school's management information system. This includes the pupil name, date of birth, pupil photograph, pupil class name, dietary preferences, 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? – Old Park School routinely shares pupil information with relevant staff within the school, schools that the pupil attends after leaving, the Local Authority, the Department for Education, Health Services, Learning Support Services, RM Integris and various third party Information Society Services applications.

Within the context of Relish School Food Ltd there is an interface with a payment system called Scopay (Tucasi). No card details are retained or held by Relish School Food Ltd, Scopay (Tucasi) entirely manages the payment processing of the transaction.

Scopay (Tucasi) does not transmit or store card details. However, they still need to maintain PCI Compliance to support the PCI compliance status of each individual school.

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. Relish will collect information medical dietary requirements.

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 Relish School Food Ltd states that the following personal data will be collected: parent/guardian, the child's name, address, date of birth, facial photograph, bank details and other data Relish School Food Ltd may seek from time to time or when a request is made for further services. Relish School Food Ltd may also ask for information if a parent/guardian report a problem with their site.

Special category data will also be collected in relation to health information, e.g. allergens and dietary information. Article 9 2 (g) of the UK GDPR sets out the conditions for the processing of special category data to be lawful. The processing of allergen and dietary information is necessary for reasons of substantial public interest, to safeguard the health of data subjects.

The information is sourced from Old Park School the management information system.

Special Category data? – Special category data will be collected in relation to health information, e.g. allergens and dietary information. 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 processing of allergen and dietary information is necessary for reasons of substantial public interest, to safeguard the health of data subjects.

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 1 to Year 14 pupils [153], and workforce [152].

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

The school provides education to its students with staff delivering the National Curriculum

What is the nature of your relationship with the individuals? – **Old Park School** collects and processes personal data relating to its pupils and employees to manage the parent/pupil and employment relationship.

Through the Privacy Notice (pupil/workforce) Old Park School is committed to being transparent about how it collects and uses data and to meeting its data protection obligation.

How much control will they have? – Relish School Food Ltd users (parents, staff) may have individual user accounts to log into the Relish app 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? – Relish School Food Ltd implement appropriate technical and organizational measures to protect Personal data against accidental or unlawful alteration or loss, or from unauthorized, use, disclosure or 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.

Old Park School has the responsibility to consider the level and type of access each user will have.

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

- **ISSUE:** The cloud based solution will be storing personal data
  RISK: There is a risk of uncontrolled distribution of information to third parties
  MITIGATING ACTION: Relish School Food Ltd implement appropriate technical and organizational measures to protect Personal data against accidental or unlawful alteration or loss, or from unauthorized, use, and disclosure or access. This includes personal data is encrypted in transit and at rest.

  Each clustered server operates up to date defence and detection systems and are additionally protected by Relish School Food Ltd externally provided Web Application Firewall WAP to reject brute force attacks. Full audit logging of all attacks and attempted access are monitored and reviewed against recognised blacklist threats via the networks. The WAP is constantly monitored and updated/patched to the latest threats as they become available. Each server utilises a suite of security tools to detect and defend against and block detected external threats

- **ISSUE**: Transfer of data between the school and the cloud
  RISK: Risk of compromise and unlawful access when personal data is transferred
  MITIGATING ACTION: The Privacy Notice for Relish School Food Ltd notes that all information Old Park School provides is stored on secure systems. The system has

different access levels and multi factor authentication. All data is encrypted using certificates in transfer and within the database - we use RSA Encryption SSL certificate for all our data transfer. All data connections and transfers are made over HTTPS RSA Encryption SSL certificate (TLS_AES_128_GCM_SHA256, 128 bit keys TLS 1.3)

Any payment transactions will be encrypted using SSL technology.

Where Relish School Food Ltd have given the school (or where the school have chosen) a password which enables access to certain parts of their site, the school is responsible for keeping this password confidential. This is not shared with anyone else

- **ISSUE:** Use of third-party sub processors?
  RISK: Non-compliance with the requirements under UK GDPR
  MITIGATING ACTION: Relish School Food Ltd use an external data centre to host their servers and databases. All Relish School Food Ltd data is securely located within their facilities based in Reading, UK. All data resides within the EEA. The facilities and staff are ISO27001 certified

  ISSUE: Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: Relish School Food Ltd servers operate on a private cluster of high-performance dedicated secure Linux servers compiled in a private cloud configuration. The cluster is hosted in a state-of-the-art tier 4 data centre located Milton Keynes & Reading, UK. Relish School Food Ltd partner with UKDedicated Ltd (ukdedicated.com) trading as GURUCLOUD (guru.co.uk). Relish School Food Ltd only provision and operate dedicated servers. The UKDedicated Centro facility holds ISO 14001 for Environmental Management System, ISO 27001 and ISO 9001 accreditations for Information Security Management and Quality Management

- **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: All Relish School Food Ltd data is securely located within their facilities based in Reading, UK. All data resides within the EEA

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Requestors have the right to ask Relish School Food Ltd not to process their personal data for marketing purposes. Relish School Food Ltd will prompt the school (before collecting your data) if we intend to use persona data for such purposes or if Relish School Food Ltd intend to disclose personal information to any third party for such purposes. The school can exercise its right to prevent such processing by checking certain boxes on the forms Relish School Food Ltd use to collect data. Schools can also exercise the right at any time by contacting us at dpo@relishschoolfood.co.uk

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Relish School Food Ltd only retain personal data whilst a child remains on the school MIS. Non-identifiable information, such as sales data for example, is retained in the system for as long as a school remains a Relish Client. Non-identifiable information is not attributable to a person or persons

- **ISSUE:** Data Back ups
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Relish-OPS runs a full back-up of the databases every 12 hours and transaction log back-ups every 15 minutes. Further full disk back-ups of all servers are completed nightly and retained for 30 days

  Additionally, databases are downloaded securely each night to our own off-site location and retained for 30 days. A copy is made on the first of each month and is retained indefinitely

Relish School Food Ltd have 3 levels of backup. The first is held at server/data-centre level and the other 2 are held remotely at local level. At the local level the data is downloaded regularly to our NAS drive and saved to 2 different secure locations: office and offsite. The servers and their access are strictly controlled and only accessed via approved and qualified data-centre technicians. Multi factor login authentication are used at server level and also at local off-site storage level. Only specified members of the Relish IT Team have access credentials. All backup data is encrypted at point of storage

All storage data is encrypted. The devices are theft-proof and fire resistant to industry standards. Each back-up device is independently configured with firewall settings that are regularly reviewed and monitored by external providers 24/7. Both the data centre and our off-site locations are in premises that are secured by physical key and electronic code entry systems with full CCTV monitoring

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: In line with Article 33 of the UK GDPR, The processor (Relish School Food Ltd) shall notify the Controller without undue delay after they become aware of a data breach. Where Relish School Food Ltd is the Data Controller, the ICO will be notified of any personal data breach without undue delay and within 72 hours of having become aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons

  A log entry is made outlining the nature of the breach, time frames, the person(s) involved and actions taken. Relish School Food Ltd will take all necessary steps to contain the breach and assess the risk of harm caused by the breach

  Where action is necessary, this will be carried out to protect those effected

  Where necessary, the Data Controller, The Commissioner and/or the Data subject will be notified of the data breach, including all information outlined in Article 33 of the UK GDPR

ISSUE: Post Brexit
RISK: UK GDPR non-compliance
MITIGATING ACTION: All Relish School Food Ltd data is securely located within their facilities based in Reading, UK. All data resides within the EEA

- **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: A Subject Access Request (SAR), is a written, signed request from a data subject to identify what personal data an organisation is processing on their behalf, why that organisation holds it, and who it is disclosed to. This right, commonly known as subject access. Relish School Food Ltd recognises the rights of the data subject under the UK GDPR

  All data associated with the Subject Access Request will be stored within Relish School Food Ltd's in-house support mechanisms, with a unique reference code for that Data Subject, and will include the initial request, e-mail correspondence and responses. This will be kept for one year, following a completed response or resolution and deleted

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Relish School Food Ltd does not share or disclose any of the school's personal information without the school's consent. Relish School Food Ltd 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: Appropriate training is undertaken by personnel that have access to the Relish app

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Personal information used in the Relish School Food Ltd platform is always kept to a minimum and is only visible by staff elected by the school. Relish School Food Ltd 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

  Relish School Food Ltd fully comply with ISO27001 Annex A.11. and where possible adhere to 27001 principles. UKDedicated Centro facility holds ISO 14001 for Environmental Management System, ISO 27001 and ISO 9001 accreditations

  Organisation name: School Catering Support Ltd, ICO Registration reference: ZA397790

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 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. Encrypted in transit and at rest	Reduced	Medium	Yes
Data Breaches	Relish School Food Ltd 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:	Miss Tina Partridge	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Miss Tina Partridge	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Yes	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: (1) Where servers are located, what are the certified security and regulations? Are the servers located behind firewalls, etc? (2) During transfer of personal data is end to end encryption used during transit? i.e. strong SHA-2/2048 bit encryption, etc? (3) What is the process of reporting a data breach which is the fault of Relish Food Ltd? (4) How is data backup? (5) Does Relish Food Ltd have industry standard certification, e.g. ISO 27001? ICO registration?		
DPO advice accepted or overruled by: Accepted by Tina Partridge 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 incorporated into section 2		
Consultation responses reviewed by: Retrospective If your decision departs from individuals' views, you must explain your reasons		
Comments: n/a		
This DPIA will kept under review by:	Tina Partridge	The DPO should also review ongoing compliance with DPIA