Data Protection Impact Assessment (Tucasi)

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 Tucasi. 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 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.

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? – To help deliver a cost effective solution to meet the needs of the business. The cloud based system will enable the school to save time spent in recording, tracking and receiving payment for school out of hour clubs, trips, school dinners, and school sundry items. Tucasi is a fully integrated software solution with a dinner money, extended day, and trip modules 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. Tucasi 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. Tucasi can be accessed by the user via mobile devices. Tucasi 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 trips 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. Tucasi can link to the school's management information system which ensures pupils records are kept up to date. Pupil data is uploaded into Tucasi using csv file generated from the school's management information system. The school can record free school meals. Meals can be recorded daily/weekly by the school office highlighting payments against the pupil and selected online by the parent/guardian. **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

Tucasi will enable the user to access information 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 legitimate 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. Tucasi obtains personal data from the school's management information system via csv file. This includes the pupil name, address, unique personal number, class and free school meals. 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.

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 Tucasi there is an interface with World Pay however personal data is not shared between the two systems.

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 Tucasi 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. Parental/guardian information will be collected relating to Parent/Guardian name, parent/guardian e-mail address, and parent/guardian contact number. It also states under the 'data minimization' principle that Tucasi will never collect any unnecessary personal data from the school and will not process school information in any way, other than that specified in the Privacy Notice for Tucasi. The information is sourced from **Hurst Green Primary School** the management information system either via manual import through csv file format. **Special Category data?** – Tucasi records whether a pupil can only eat Halal which would imply the religion of the child. Similarly information relating to health concerning allergies is also recorded on Tucasi. This falls under the GDPR special category data. **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 its data retention policy. **Scope of data obtained?** – How many individuals are affected (pupils, workforce, governors, volunteers)? And what is the geographical area covered? EYFS and Year 1 to Year 6 pupils 424 and workforce 50.

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?** – **[insert Name of 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?** – Tucasi users (parents, staff) may have individual user accounts to log into Tucasi to retrieve information. **Do they include children or other vulnerable groups?** – None of the data is classified under 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 Tucasi's Secure Data Centre, this data is encrypted in transit using TLS 1.2, and subsequently stored at rest within an encrypted database. In terms of data backups Tucasi uses Amazon Web Services which is certificated to certain security and regulations including ISO 27001 and PCI Data Security Standard. In terms of application security, users (staff) can log into the Tucasi IOS and android mobile applications and view user specific data. Tucasi 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: Tucasi Ltd use appropriate measures to safeguard personally identifiable information, which measures are appropriate to the type of information maintained, and follows applicable laws regarding the safeguarding of any such information under the control of Tucasi. Encryption technology may be used to enhance information privacy and help prevent loss, misuse, or alteration of the information under the control of Tucasi Ltd. Servers are located in an ISO 27001 certified data centre within the UK, all of our 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: Tucasi Ltd Privacy Notice states that it follows generally accepted industry standards to protect the personal data submitted to Tucasi Ltd, both during transmission and once received. Encryption technology is used to enhance information privacy and prevent loss, misuse, or alteration of the information under the control of Tucasi Ltd

- **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: Tucasi is attested as PCI Compliant and has created an ISO27001 ISMS and hope to obtain certification by Autumn 2019

- **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: Tucasi Ltd do not share personal data outside of the EEA

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: GDPR non-compliance
  MITIGATING ACTION: Tucasi's Privacy Notice states that the school, and for that matter the parent/guardian, has a right to access any personal information that Tucasi processes including what personal data is held, the purposes of the processing, categories of personal data concerned, recipients to whom the personal data has/will be disclosed, how long Tucasi stores the information, and information about the personal data source. If Tucasi receives a request from the school to exercise any of these rights, Tucasi may ask the school to verify its identify before acting on the request; this is to ensure that the data is protected and kept secure

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: GDPR non-compliance
  MITIGATING ACTION: The personal data will be managed in line with the school's data retention policy. Tucasi Ltd only ever retains personal information for as long as is necessary. Tucasi Ltd actively reviews its Privacy Policy to meet these obligations. Tucasi Ltd will keep school data on its systems for as long as a relationship exists between the school and Tucasi Ltd

- **ISSUE:** Data Back ups
  RISK: GDPR non-compliance
  MITIGATING ACTION: Tucasi use Amazon Web Services (AWS) back up services. AWS back up is a fully managed, policy based back up solution that makes it easy to automatically back up the Tucasi application data across AWS services in the cloud

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

  MITIGATING ACTION: Tucasi Ltd also employs industry-standard measures and processes for detecting and responding to inappropriate attempts to breach Tucasi Ltd systems. In the event of a data breach, Tucasi Ltd will notify the personal data breach to the school

- **ISSUE:** No deal Brexit
  RISK: GDPR non-compliance
  MITIGATING ACTION: Tucasi services are hosted within the UK, subsequently there are no major concerns with the possibility of a No Deal Brexit. No data leaves the EU and all core services remain within the UK.

- **ISSUE:** Subject Access Requests
  RISK: The school must be able to retrieve the data in a structured format to provide the information to the data subject
  MITIGATING ACTION: Where Tucasi Ltd are acting as the data processor, they will refer any request from an individual for access to personal information which is held to the school. All data forming part of the Subject Access Request can be exported to.csv format through Excel. Tucasi Ltd will not respond directly to the request.

- **ISSUE:** Data Ownership
  RISK: GDPR non-compliance
  MITIGATING ACTION: Tucasi does not share or disclose any of the school's personal information without the school's consent. Tucasi 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 GDPR compliance

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

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

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 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 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
No deal Brexit	Possible	Significant	Medium
Subject Access Request	Probable	Significant	Medium
Data Retention	Probable	Significant	Medium

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no
Data Transfer	Secure network, end to end encryption	Reduced	Medium	Yes
Asset protection & resilience	Data Centre in EU. Accredited to ISO 27001 and PCI Data Security Standard	Reduced	Medium	Yes
Data Breaches	Tucasi's ability to respond and deal with a data breach	Reduced	Low	Yes
No deal Brexit	Tucasi servers are hosted within the UK	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:	**Mrs V Kelly**	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	**Mrs V Kelly**	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) What is the cloud based solution chosen where data processing/storage premises are shared?, i.e. where are servers located, what are the certified security and regulations? Are the servers located behind firewalls? Servers are located in an ISO 27001 certified data centre within the UK, all of our servers are protected by physical firewalls

(2) 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? Data is received by API end points hosted in Tucasi's Secure Data Centre, this data is encrypted in transit using TLS 1.2, and subsequently stored at rest within an encrypted database

(3) Location of servers hosting personal data? No data leaves the EU and all core services remain within the UK

(4) Contingency arrangements around a no deal Brexit? Tucasi services are hosted within the UK, subsequently there are no major concerns with the possibility of a No Deal Brexit

(5) Does Tucasi Ltd have industry standard certification, e.g. ISO 27001? Tucasi is attested as PCI Compliant and has created an ISO27001 ISMS and hope to obtain certification by Autumn 2019

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:	**Mrs V Kelly**	If your decision departs from individuals' views, you must explain your reasons
Comments: **[Comments provided]**		
This DPIA will kept under review by:	**Mrs R Whitehouse**	The DPO should also review ongoing compliance with DPIA