Data Protection Impact Assessment (GovernorHub)

Thorns Primary School operates a cloud based system. As such Thorns 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.

Thorns Primary School recognises that moving to a cloud service provider has a number of implications. Thorns 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.

Thorns 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? – To help deliver a cost effective solution to meet the needs of the business. The cloud based system will improve accessibility and ensure information security when working remotely.

The Local Authority has adopted GovernorHub to manage the Governor, Local Authority, and School relationship. Schools can access GovernorHub in their own right.

Maintained Schools/Multi Academy Trusts

Noticeboard – GovernorHub enables a school to host all e-mail addresses and post an item on the Noticeboard or e-mail relevant committees with key information.

Store documents – Manages version control ensuring Governors have access to the latest document or policies. GovernorHub hosts school documents all in one place which are easily searchable. For the more confidential items, access can be restricted on a need to know basis.

Governor News – Enables schools to keep up to date with local and national education news.

Security as standard – All school data and documents are encrypted and transported securely over the Internet. GovernorHub also aims to meet industry best practice in terms of password storage, etc.

Meeting calendar – GovernorHub has a single calendar that schools can sync to its various devices.

Clerking tools – GovernorHub has a number of tools that assists the process of clerking This includes keeping track of the constitution, committees and roles, and automatically notifying school local Governor Support Services of any membership changes.

Mobile and tablet apps – GovernorHub has apps for smartphones and tablets allowing the school to access GovernorHub and school documents on the move, or even offline.

Thorns 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. Scalability
2. Reliability
3. Resilience
4. Delivery at a potentially lower cost
5. Supports mobile access to data securely
6. Update of documents in real time
7. Good working practice, i.e. secure access to sensitive files

The 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 and workforce data in the cloud.

Step 2: Describe the processing

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

The Privacy Notice (governors and volunteers) for the school provides the lawful basis of why the school collects data.

How will you collect, use, store and delete data? – The information collected by the school is retained on the school's computer systems and in paper files. The information is retained according to the school's Data Retention Policy.

In terms of Governor information this will be managed and retained in GovernorHub.

What is the source of the data? – Information is obtained from an application process made by those who wish to serve on the school's Governing Body.

Will you be sharing data with anyone? – Thorns Primary School routinely shares governor information with other members of staff where relevant.
Thorns Primary School routinely shares governor information internally with the Local Authority, and the Department for Education.

What types of processing identified as likely high risk are involved? – Transferring 'special category' data from the school to the cloud. Storage of personal and 'special category 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? – Governor data relates to name and e-mail address, any information the school chooses to provide respecting their Governors such as address, phone number(s), date of birth, ethnicity, health, etc.

Special Category data? – GovernorHub will not be used to process special category data other than that relating to Governors. This may include ethnicity and health related data.

How much data is collected and used and how often? – In terms of GovernorHub the data collected may include a Governors name and e-mail address, any information the school chooses to provide respecting their Governors such as address, phone number(s), date of birth, ethnicity, health, etc.

The school(s)/ academies/trust at which a Governor is registered. What type of governor/trustee they are (e.g. parent, co-opted, local authority). The dates of the Governors term of office. The Governors role on the governing board (e.g. chair, vice-chair).

Whether the Governor has administrator access rights to use GovernorHub. Declarations of interest as a governor or trustee. Training records a Governor may have entered on GovernorHub. Anonymised information about the Governor's use of GovernorHub.

How long will you keep the data for? – The subscribers to the system, as data controllers, have full access to create, update and delete the data under their control. The subscribers can obtain copies of their data in a portable format at any time and can revoke user access and delete users at any time.

When a user subscription to GovernorHub expires, Ortoo Technologies Ltd will delete any remaining user data within an agreed lapse period at the end of the subscription term.

The data retention period will be documented in the school's data retention policy.

Scope of data obtained? – How many individuals are affected (pupils, workforce, governors, and volunteers)? Board of Governors 9.

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)?

What is the nature of your relationship with the individuals? – Thorns Primary School collects and processes personal data relating to its governors to manage the governor/school relationship.

Through the Privacy Notice (Governors/Volunteers) Thorns 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? – GovernorHub processes personal data on the basis of contractual obligation to subscribers, usually schools, academies, trusts, local authorities and other organisations which purchase subscriptions to the service. Ortoo Technologies Ltd is the data processor on behalf of its subscribers, who are the data controllers.

Access to the files will be controlled by username and password. GovernorHub (Ortoo Technologies Ltd) is hosting the data and has the ability to access data on instruction of Thorns Primary School who is the data controller for the provision of supporting the service.

The school will be able to upload personal data from its PC for the data to be stored remotely by a service provider. Changes made through the browser when accessing GovernorHub will update the data stored by the school.

Do they include children or other vulnerable groups? – GovernorHub will not be used to process special category data other than that relating to Governors. This may include ethnicity and health related data.

Are there prior concerns over this type of processing or security flaws? – All data is encrypted in GovernorHub. Data transfer is secured by TLS/HTTPS.

Thorns 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 including sensitive information **RISK:** There is a risk of uncontrolled distribution of information to third parties. **MITIGATING ACTION:** Ortoo Technologies Ltd use sub-processors to provide data
centre and infrastructure services as follows: Amazon Web Services, Google Cloud Platform, Microsoft Azure and Object Rocket/Rackspace
GovernorHub processing takes place in sub-processor data centres within the European Economic Area (EEA) in Dublin, South Wales and London
The staff and any contractors at Ortoo Technologies Ltd are trained in data protection and receive regular refresher training. Privileged access rights are tightly controlled and recorded.
The company employs a Data Protection Officer

- **ISSUE**: Transfer of data between the school and the cloud
  RISK: Risk of compromise and unlawful access when personal data is transferred.
  MITIGATING ACTION: Data within the GovernorHub system is encrypted during transit using TLS/HTTPS and is encrypted at rest on the GovernorHub database

- **ISSUE:** Use of third party sub processors?
  RISK: Non compliance with the requirements under UK GDPR
  MITIGATING ACTION: GovernorHub engage third party data processors for carrying out processing activities in respect of the school's personal data. GovernorHub. Ortoo Technologies ensure that these data sub processers UK GDPR compliant

  GovernorHub data centre providers, Google, Amazon, Microsoft and Rackspace all hold ISO27001 certification (copies of which can be provided on demand)

- **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage.
  MITIGATING ACTION: Access to GovernorHub infrastructure, including access and audit logs is limited to GovernorHub developers. Underlying operating systems and container images are regularly updated in accordance with supplier recommendations

- **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: The servers hosting GovernorHub are located within the EU. Data processing takes place in sub-processor data centres within the European Economic Area (EEA) in Dublin, South Wales and London

  ISSUE: Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: UK GDPR non-compliance

MITIGATING ACTION: GovernorHub is an ICO registered company (reg no Z361299X), fully compliant with UK GDPR data security handling and reporting

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
- **MITIGATING ACTION:** The subscribers to the system, as data controllers, have full access to create, update and delete the data under their control. The subscribers can obtain copies of their data in a portable format at any time and can revoke user access and delete users at any time

  When a user subscription to GovernorHub expires, Ortoo Technologies Ltd will delete any remaining user data within an agreed lapse period at the end of the subscription term

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: GovernorHub, under Ortoo Technologies Ltd, is an ICO registered company, fully compliant with UK GDPR data security handling and reporting

- **ISSUE:** Data is not backed up
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Backups are maintained through daily snapshots of the database, which are periodically tested for recovery. Additionally GovernorHub take copies of database changes which can be used for granular level recovery and instant recovery. The recovery processes are periodically tested. Records are kept of all data processing activities

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Post Brexit the UK will be outside of the European Economic Area ("EEA") at the time of exit. With regards to GovernorHub use of servers in Ireland, the UK will transitionally recognise all EEA states, EU and EEA institutions, and Gibraltar as providing an adequate level of protection for personal data. This means that personal data can continue to flow freely from the UK to these destinations following the UK's exit from the EU

As a further contingency in the event of any currently unforeseen scenario, GovernorHub could be hosted through sub processor data centres in South Wales and London

- **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: GovernorHub has the functionality to handle and respond to Subject Access Requests

  Data Controllers are able to download data on demand in response to subject access requests (SARs). Ortoo Technologies Ltd can assist with SAR data identification and download requests

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The operators of GovernorHub, Ortoo Technologies Ltd, act as a data processor on behalf of the schools, multi-academy trusts, charities, local authorities and independent organisations which subscribe to use the GovernorHub system as data controllers. GovernorHub data processing is conducted on the basis of contractual obligation to data controllers who are subscribing to use system

- **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: As a service, GovernorHub is UK GDPR compliant. The data processor remains accountable for the data within the system. The school data is not shared with any other organisation

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

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: GovernorHub data centre providers, Google, Amazon, Microsoft and Rackspace all hold ISO27001 certification (copies of which can be provided on demand)

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

  Ortoo Technologies Ltd is an ICO registered company (reg no Z361299X)

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:

- Scalability
- Reliability
- Resilience
- Delivery at a potentially lower cost
- Supports mobile access to data securely
- Update of documents in real time
- Good working practice, i.e. secure access to sensitive files

Step 3: Consultation process

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

The views of senior leadership team and the Board of Governors will be obtained. Once reviewed the views of stakeholders will be taken into account

The view of YourIG has also been engaged to ensure Data Protection Law compliance

Step 4: Assess necessity and proportionality

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

The lawful basis for processing personal data is contained in the school's Privacy Notice (Governors and Volunteers). 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
Post Brexit (GDPR noncompliance)	Possible	Significant	Medium
Subject Access Request	Probable	Significant	Medium
Data Retention	Possible	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, Certified, Penetration Testing and Audit	Reduced	Medium	Yes
Data Breaches	Documented in contract and owned by school	Reduced	Low	Yes
Post Brexit	Brexit contingency plans to relocate servers to 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:	Rebecca Jordan	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Rebecca Jordan	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: When a user subscription to GovernorHub expires, Ortoo Technologies Ltd will delete any remaining user data within an agreed lapse period at the end of the subscription term YourIGDPO Service would recommend this is stipulated in any contract with Ortoo Technologies Ltd		
DPO advice accepted or overruled by: No If overruled, you must explain your reasons		
Comments: DPO Advice provided		
Consultation responses reviewed by: N/A If your decision departs from individuals' views, you must explain your reasons		
Comments:		
This DPIA will kept under review by: Karen Cartwright The DPO should also review ongoing compliance with DPIA		