Data Protection Impact Assessment (GovernorHub)

The Earls High School ('the school'), comprising the member schools and central team, operates a cloud-based system. As such the Trust 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.

The School recognises that moving to a cloud service provider has a number of implications. The Trust 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 Trust has to its data. The location of the cloud is important to determine applicable law. The Trust 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 are upheld by the Trust.

The 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 organisation. The cloud-based system will improve accessibility and ensure information security when working remotely.

The School has adopted GovernorHub to manage documentation for the Trust Board and local governing bodies. GovernorHub enables the Trust Board, local governing bodies, school and central team users, and clerks to communicate and store membership details, training records, meeting schedules and papers, and other documents and information in a secure and accessible place.

Noticeboard – GovernorHub enables a school or trust 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 members, directors and governors have access to the latest document or policies. GovernorHub hosts school and trust documents all in one place, making them easily searchable. For the more confidential items, access can be restricted on a need-to-know basis.

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

Security as standard – All school and trust 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 and trusts can sync to its various devices.

Clerking tools – GovernorHub has a number of tools that assist the process of clerking. This includes keeping track of the constitution, committees and roles.

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

Local Governing Body Areas – Each local governing body, plus the Trust Board, have an area on GovernorHub (see the features above). Members of the local governing body can only see their papers and details, but members and directors of the Trust Board can see the papers and details for schools in the Trust.

Shared news, calendar and resources – Trusts can store resources that all of the member schools' local governing bodies can access, send them news and information and see every meeting across the trust on a shared calendar.

Large MATs – For larger MATs and academy chains GovernorHub provide database access. Manage the list of governors, members and directors across the whole MAT or chain.

The Trust will undertake the following processes:

1. Collecting personal data
2. Recording and organising 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 Trust aims to achieve the following:

1. Scalability
2. Reliability
3. Resilience
4. Efficiency: one platform for registered users to upload and access information
5. Consistency: the same platform used by all member schools and the central team

6. Delivery at a potentially lower cost
7. Supports mobile access to data securely
8. Update of documents in real time
9. Good working practice, i.e. secure access to sensitive files
10. Fulfilment of governance audit requirements: The Trust Board and Executive Team have oversight of local governing body work through the documents and information shared on GovernorHub.

The cloud service provider cannot do anything with the Trust's data unless they have been instructed by the Trust. The Trust's Privacy Notices 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 individual member schools;(Members and Directors) for the Trust Board) provides the lawful basis of why the Trust collects data.

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

Information about members, directors and governors will be managed and retained in GovernorHub.

What is the source of the data? – Information is obtained from an application process undertaken by those who wish to serve on a local governing body or the Trust Board.

Will you be sharing data with anyone? – The Trust routinely shares member, director and governor information with other members of staff where relevant.

The Trust routinely shares governor information with the Local Authority (where applicable) and the Department for Education.

What types of processing identified as likely high risk are involved? – Transferring 'special category' data from the Trust 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? – Member, director and governor data relates to name and e-mail address, any information the Trust chooses to provide about its members, directors and governors such as address, phone number(s), date of birth, ethnicity, health, etc.

Special Category data? – Some of the personal data collected falls under the UK GDPR special category data. 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 names and e-mail addresses of members, directors and governors, as well as any information the Trust chooses to provide about them, such as home address, phone number(s), date of birth, ethnicity, health, etc.

The school at which the individual serves on the local governing body. What type of governor they are (e.g. parent, co-opted, local authority). The dates of directors' and governors' terms of office. Directors' and governors' role on the Trust Board or local governing body (e.g. chair, vice-chair).

Whether the member, director or governor has administrator access rights to use GovernorHub. Declarations of interest as a member, director or governor. Training records a member, director, governor or clerk may have entered on GovernorHub. Anonymised information about the use of GovernorHub by members, directors and governors.

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 Trust's data retention policy.

Scope of data obtained? – Nine governors Local Governing Body of The Earls High School

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? – The Trust collects and processes personal data relating to its members, directors and governors to manage the member, director, governor and Trust/school relationship.

Through the Privacy Notice ((Members and Directors) and (Governors/Volunteers)) the Trust 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 the Trust, who is the data controller for the purpose of supporting the service.

The Trust will be able to upload personal data from its PCs 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 Trust.

Do they include children or other vulnerable groups? – GovernorHub may be used to process special category data other than that relating to members, directors and governors. This may include ethnicity and health-related data presented in reports on pupils or staff that form part of papers considered at Trust Board or local governing body meetings. Data will be anonymised and aggregate numbers will typically be used.

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.

The Trust recognises that moving to a cloud-based solution raises a number of General Data Protection Regulation 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 Trust's personal data. GovernorHub (Ortoo Technologies Ltd) ensure that these data sub-processors are UK GDPR compliant.

  GovernorHub data centre providers, Google, Amazon, Microsoft and Rackspace, all hold ISO 27001 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 in relation to 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 is now outside of the European Economic Area ("EEA"). With regard to GovernorHub use of servers in Ireland, the UK will 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 flow freely from the UK to these destinations.

  As a further contingency GovernorHub could be hosted through sub-processor data centres in South Wales and London.

- **ISSUE:** Subject Access Requests
  RISK: The Trust 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 Trust 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 Trust 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 ISO 27001 certification (copies of which can be provided on demand).

ISO 27001: is one of the most widely recognised, internationally accepted independent security standards. GovernorHub has earned ISO 27001 certification for the systems, applications, people, technology, processes, and data centres 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 Trust's moving to a cloud-based solution will realise the following benefits:

- Scalability
- Reliability
- Resilience
- Efficiency: one platform for registered users to upload and access information
- Consistency: the same platform used by all member schools and the central team
- 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
- Fulfilment of governance audit requirements: The Trust Board and Executive Team have oversight of local governing body work through the documents and information shared on GovernorHub.

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 teams, the Trust Board and local governing bodies 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 Trust's Privacy Notices ((Governors and Volunteers) for the member schools and (Members and Directors) for the Trust Board). 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 Trust 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 Trust will remain 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	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 Trust	Reduced	Low	Yes
Subject Access Request	Technical capability to satisfy data subject access request	Reduced	Low	Yes
Data Retention	Implementing Trust data retention periods in the cloud	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	**Name/date**	**Notes**
Measures approved by:	Stour Vale Academy Trust	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Stour Vale Academy Trust	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: Accepted

If overruled, you must explain your reasons

Comments: DPO advice provided

Consultation responses reviewed by: Stour Vale Academy Trust central and executive team

If your decision departs from individuals' views, you must explain your reasons

Comments: Members, directors and governors were notified by email and in Trust Board and local governing body meetings of the intention to subscribe to GovernorHub to realise the benefits detailed above. Verbal feedback was sought and, on the basis of the feedback received, the decision was taken to subscribe.

This DPIA will kept under review by:

Stour Vale Academy Trust Operations Officer

The DPO should also review ongoing compliance with DPIA.