Data Protection Impact Assessment (Talent Link)

Thorns Primary School uses Talent Link which sits on a remote server. 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 the use of Talent Link 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 Talent Link 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 server is important to determine applicable law. The school will need to satisfy its responsibilities in determining whether the security measures the service 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. Talent Link is an applicant tracking system used by schools to support their end to end recruitment process needs. These include CRM, job approvals, job posting, social media integration, career site development, applying online, selection process management including shortlisting, assessment integration, interview scheduling, offers and contract generation and onboarding.

Features of Talent Link include the following:

- Applicant tracking, candidate management, recruitment CRM and campaign management
- Job requisition and approval management
- Job distribution
- Career sites, chat bot's, configurable application processes & CV parsing
- Talent Pooling, pipeline management & candidate search and match
- Manager Self Service including dedicated dashboards & online short-listing
- Interview scheduling and two-way calendar integrations
- Offer & eSignatures via DocuSign
- Creation of engaging pre and on-boarding experiences
- Interactive recruitment metric dashboards and ad-hoc reporting

Talent Link will improve accessibility and ensure information security when working within the school and remotely.

Thorns Primary School will undertake the following processes:

- Collecting personal data
- Recording and organizing personal data
- Structuring and storing personal data
- Copying personal data
- Retrieving personal data
- Deleting personal data

By opting for Talent Link the school aims to achieve the following:

- Scalability and performance
- Configurability (customer is in control of the design)
- Data security
- Reliability and Resilience
- Delivery at a potentially lower cost (i.e. task and reminders help reduce time to hire)
- Supports mobile access to data securely (with Talent Link's mobile app)
- Update of documents in real time
- Good working practice, i.e. secure access to sensitive files

Talent Link is hosted on a remote server with secure access via user name and login relevant to the school.

Talent Link will automatically archive job applications/candidate data after 6 months dependent on the recruitment.

Talent Link cannot do anything with the school's data unless they have been specifically instructed by the school. The schools Privacy Notice (Workforce) will be updated especially with reference to the storing of personal data in Talent Link.

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(s) for (Workforce) for the school provides the lawful basis of why the school collects data.

How will you collect, use, store and delete data? – Information will be collected from the candidate by the candidate setting up an individual account and Talent Link generating a unique password for the candidate to access their account. Information will be stored remotely on the Talent Link server.

Information will be retained on Talent Link in line with the school's data retention policy.

What is the source of the data? – Information held on Talent Link is obtained from information obtained from the candidates' application form which is submitted online or via a manual application form submitted to the school. It will also contain information generated by Talent Link to include candidate ID, application created date, the application updated date, requisition ID of the request the candidate applied to, any notes made by other users against the candidate record.

In terms of the interview process personal data will be generated through the candidate interview feedback, date of the feedback, username of the user who provided the feedback,

Alternatively this process may be conducted by the school manually and outside of Talent Link.

Will you be sharing data with anyone? – Thorns Primary School routinely shares workforce information internally with people responsible for HR and recruitment (including payroll), senior staff, with the Local Authority, and the Department for Education.

What types of processing identified as likely high risk are involved? – 'Special category' data from the school is transferred securely to the server which is located remotely. Storage of personal and 'special category data in Talent Link.

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?

– *Personal data*: Relates to information (such as name, address and contact details, including e-mail address and telephone number). Details of criminal records. It will also include details of qualifications, skills, experience and employment history , (including start and end dates with previous employers and with the school). It may also include employee or teacher number, and marital status. Special categories of data (such as gender, age, ethnic group).

Candidate information: Interview notes, application history, rating, candidates name, Email address, candidate profile date, candidate last updated date, phone numbers, address, Talent Link candidate ID, application created date, the application updated date, requisition ID of the request the candidate applied to, name of the requisition the candidate applied to, any notes made by other users against that candidate record, username of the user who made that note, candidate interview feedback, date of the feedback, username of the user who provided the feedback, interview type.

Recruiter information: This data includes candidate name, candidate contact information, company, status, source, last application date, action taken date, application notes, candidate current job details, application URL, candidate status history and dates, reason for rejection, outcome information related to interviews (including feedback and resulting recommendations) and other general candidate feedback.

The above data may also be collected manually and entered onto Talent Link.

Special Category data? – Some of the personal data collected falls under the UK GDPR special category data. This includes race; ethic origin; religion; sexual orientation, trade union membership, and health.

How much data is collected and used and how often? – Personal data is collected for the purpose of recruitment.

How long will you keep the data for? – All relevant information should be added to the workforce file. Information on unsuccessful candidates will be retained for a minimum of 6 months and no longer than 1 year in line with the schools data retention policy.

Scope of data obtained? – How many individuals are affected? And what is the geographical area covered?

Relates to the recruitment to the school and the number of vacancies in anyone year.

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? – Thorns Primary School collects and processes personal data relating to future employees. Thorns Primary School needs to process personal data to assist in the process of recruitment.

Through the Privacy Notice (Workforce) 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? – Access to data supporting the recruitment process will be controlled by username and password. As part of the recruitment process candidates will have access to their personal data via their candidate home page. Under UK GDPR candidates have the option to exercise their right to be forgotten. This right also applies if their applications have been uploaded by the school.

However, under data protection law Thorns Primary School recognizes that individuals can exercise certain rights and as such the school will be fully compliant with such laws.

Do they include children or other vulnerable groups? – No.

Are there prior concerns over this type of processing or security flaws? – No.

Thorns Primary School recognises that moving to a cloud based solution raises a number of UK 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: Talent Link have implemented a control framework based upon market standards as ISO27001/2, and CobIT (Control Objectives for Information and Related Technology). The effectiveness of this control framework is audited by LRQA (Lloyds Register Quality Assurance) and PwC and evidenced in the form of the ISO 27001 certificate. Talent Link have a Chief Privacy Officer/Data Protection Officer who works with all departments to ensure the framework is robustly adhered to

- **ISSUE**: Transfer of data between the school and the cloud
  RISK: Risk of compromise and unlawful access when personal data is transferred.
  MITIGATING ACTION: Transport Layer Security (TLS) (version 1.2 or above) is used to protect data in transit. All data is encrypted at rest and in transit to AES (Advanced Encryption Standard) 256 standard

- **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage.
  MITIGATING ACTION: Physical access control, complying with SSAE (Statement on Standards for Attestation Engagements) -16 /ISAE (International Standard for Assurance Engagements) 3402. Host Intrusion Detection Systems (HIDS). AWS (Amazon Web Services) Shield and AWS Guard duty. DDOS (Distributed Denial of Service) protection and intelligent threat detection. Third-party scanning of application and infrastructure. OWASP ZAP is built-in the deployment process

- **ISSUE:** Disaster recovery
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: In the event of a disaster within a data centre used for the delivery of the Solution, the Company will initiate its Disaster recovery procedure. The

Company shall ensure that replicated data and other assets shall be available to support Disaster Recovery within the respective hosting country used for production service delivery. Data shall not be exported from the hosting country to support Disaster Recovery. In the event of a Disaster, recovery time is expected to be less than 24 hours and recovery point is expected to be less than 1 hour. The procedures for Disaster Recovery are tested by the Company once a year. The Company is certified against ISO 22301 for Business Continuity

- **ISSUE:** System back up
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Full database backups are performed daily, weekly, and monthly. File stores are held on high availability storage infrastructures and backups are automatically taken and secured independent of a single data centre location. Backup generations are retained for six months throughout the Agreement and for six months from the termination date of the Agreement. All data backups shall remain within the country used for hosting and secured by encryption to AES-256 standard

- **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 solution is hosted in the UK

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Talent Link has a two factor authentication process which limits access to the Back Office of Talent Link via registered IP addresses

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
- **MITIGATING ACTION:** The Terms and Conditions of the data processor undertakes to comply with the obligations under relevant and applicable data protection laws, principles and agreements

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Users of Talent Link can report incidents via the Customer Portal 24/7, or via telephone 8 am - 6pm UK time. A case will be raised on Talent Link's portal and the customer will be provided with regular updates, both via the portal and the telephone. If there is a common incident affecting a number of customers this will be highlighted on the login page of the portal. There are predefined response times to different levels of the incident outlined in the Service Level Agreement. Major Incident Reports will be distributed once a major incident has been resolved

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

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The school remains the data controller. Talent Link is the data processor and **Thorns Primary School** and Dudley MBC is the joint data controller. Please see Terms and Conditions.

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

- **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: The Terms and Conditions state that the Company is a data processor and the Customer is the data controller. The parties shall comply with their

respective statutory data protection obligations. The Company agrees that it will only process data on behalf of, and in the name of, the Customer

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

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Talent Link complies with a recognised standard (CSA CCM version 3.0). Penetration testing is undertaken at least once a year. Penetration testing approach is performed by a Tigerscheme qualified provider or CREST approved service provider. ISO/IEC 27001 certification

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 Talent Link will realise the following benefits:

- Scalability and performance
- Configurability (customer is in control of the design)
- Data security
- Reliability and Resilience
- Delivery at a potentially lower cost (task and reminders help reduce time to hire)
- Supports mobile access to data securely (with Talent Link's mobile app)
- 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 (Workforce). The lawful basis includes the following:

6.1(b) Processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
6.1(c) Processing is necessary for compliance with a legal obligation to which the controller is subject

For example: The Health and Safety at Work Act, Equality Act 2010, The Disability Discrimination Act.

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

9.2 (b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

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, ISO 27001	Reduced	Medium	Yes
Data Breaches	Documented in contract and owned by school	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		
DPO advice accepted or overruled by: **No** If overruled, you must explain your reasons		
Comments:		
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