Data Protection Impact Assessment (Tribepad)

Summerhill School uses Tribepad which sits on a remote server. As such Summerhill 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.

Summerhill School recognises that the use of Tribepad has a number of implications. Summerhill 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 Tribepad 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.

Summerhill 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. Tribepad is an applicant tracking system used by schools to support their end to end recruitment process needs. This will be provided through the West Midlands Employers. 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.

Tribepad will allow Summerhill School to update its recruitment processes and enhance the recruitment experience for hiring schools and applicants allowing Summerhill School to recruit more efficiently. The application tracking system enables the school to have more control over how they recruit. Benefits for the applicants include an individual profile with access to a recruitment portal through Tribepad for ease of application.

Features of Tribepad include the following:

The self service portal

Enables potential candidates to:

- Search and apply for jobs
- Review applications
- Set smart alerts
- View application progress
- Track referrals
- Communicate with recruiters
- Access resources

The job advert

- Accessible and mobile friendly

- Social media apply and CV import
- Candidate progress tracking
- Automated candidate comms
- Full branding with media
- Application journeys tailored to roles

The candidate

- Bulk or individual interview invites
- Optional candidate self booking
- Individual or group interview slots
- Office 365 and GCal calendar integration
- Automated reminders and prompts
- Instant integration of Tribepad interviewing
- Interview workflow builder

The recruiter

- Mobile friendly, self-service manager dashboard
- Automatic alerts, reminders, and updates
- Workflows
- Short candidate factsheets to show highlights

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

Summerhill 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 Tribepad 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 Tribepad's mobile app)
- Update of documents in real time
- Good working practice, i.e. secure access to sensitive files

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

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

Tribepad 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 Tribepad.

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?

Job vacancy details will be posted on to Tribepad including Job Descriptions and Person Specifications and made publicly available to view for prospective applicants. Successful applicants' pre-employment checks will be processed via Tribepad. References for the applicant will be sent through the Tribepad system. Details of the pre-employment checks received will be shared with the school before a formal offer is made to the applicant to check everything is in order.

The Tribepad system will generate offer letters which are emailed to the successful candidate who will then use the portal to accept the offer. At this stage, the platform will then request references from the candidate and consent to contact them. For schools, in order to keep within the KCSiE guidance, schools will be made of the reference alerts in the first instance, so that they can check for gaps in employment. If approved by the school, the alerts are then sent onto the referees or additional reference requests can be made.

The Privacy Notices (pupil) for the school provides the lawful basis of why the school collects data. The lawful basis in order to process personal data in line with the 'lawfulness, fairness and transparency principle is as follows:

6.1 (c) Processing is necessary for compliance with a legal obligation to which the controller is subject; e.g. health & safety and safeguarding

6.1 (e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

6.1 (f) Processing is necessary for the purposes of the legitimate interest pursued by the controller or by a third party

The lawful basis for collecting special category information relates to Article 9 2 (g) *processing is necessary for reasons of substantial public interest and is authorised by domestic law.*

The school has considered the lawful basis by which it processes personal data. This is recorded in Summerhill School Privacy Notice (Pupil) and where appropriate in Privacy Notice (Workforce).

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 Tribepad generating a unique password for the candidate to access their account. Information will be stored remotely on the Tribepad server.

Information will be retained on Tribepad in line with the school's data retention policy. All details are automatically archived after six months in line with GDPR. Individuals who have a created profile on the portal but have not interacted with it for a period of twelve months, will be alerted to see if they wish to retain their profile for a further twelve months, otherwise the account will be automatically removed.

What is the source of the data? – Information held on Tribepad 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 Tribepad 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 Tribepad.

Will you be sharing data with anyone? – Summerhill 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 Tribepad.

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?

Data collected is in line with school policy in regard to pre-employment checks including Right to Work in the UK, cleared DBS certificate (or Risk Assessment if positive result). Medical Assessment with any reasonable adjustments needed, photo identification and verification of home address will be stored on the school's management information system.

This is stored in Tribepad through the recruitment process before being moved to the school's management information system once recruitment has commenced- all data retained in Tribepad is auto- archived after six months.

This is the same process for all applicants regardless of where they are applying from.

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, application created date, the application updated date, requisition ID of the request the candidate applied to, name of the requisition the candidate applied to, 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 Tribepad.

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.

The lawful basis for collecting special category information relates to Article 9 2 (g) *processing is necessary for reasons of substantial public interest and is authorised by domestic law.*

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)?

In terms of recruitment the candidate has full control over what personal data is supplied to the school, but any information not supplied may delay their recruitment. Applicants will expect the school to collate pre-employment documentation as part of their recruitment process- this does not include children or vulnerable groups.

There are not prior concerns or data flaws that the school know of. This is a standard recruitment process.

What is the nature of your relationship with the individuals? – Summerhill School collects and processes personal data relating to future employees. Summerhill School needs to process personal data to assist in the process of recruitment.

Through the Privacy Notice (Workforce) Summerhill 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 Summerhill 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.

Summerhill 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: Tribepad have implemented a control framework based upon , internationally accepted independent security standards ISO27001. As such there are hardware and software firewalls protection Application Protocol Interfaces and servers

  Cloud platform has rigorous maintenance schedule which meets the security standards of ISO 27001

  Tribepad have independent penetration testing quarterly and some of Tribepad's customers also do their own penetration testing against the platform.

- **ISSUE**: Transfer of data between the school and the cloud
  RISK: Risk of compromise and unlawful access when personal data is transferred.
  MITIGATING ACTION: User interactions protected by SSL sessions.

  Tribepad use industry standard AES256 encryption

- **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 compliant with the standards as set out by ISO 27001

- **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, compliance with ISO 27001 ensures that there is a disaster recovery procedure in place. 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

- **ISSUE:** System back up
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Compliance with ISO 27001 which is one of the most widely recognized, internationally accepted independent security standards ensure that there is a full database backup 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.

- **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: Industry best-practice password management enforced

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
- **MITIGATING ACTION:** Tribepad's functionality can reflect and enable the school to implement the data retention periods as documented in the school's Privacy Notice

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Industry best-practice password management enforced

- **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: Tribepad 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. Tribepad is the data processor and Summerhill School and Dudley MBC is the joint data controller. Please see Terms and Conditions

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Tribepad personal data stored at UK data centres which is ISO27001-compliant

- **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: Tribepad have implemented a control framework based upon , internationally accepted independent security standards ISO27001. As such there are hardware and software firewalls protection Application Protocol Interfaces and servers

Cloud platform has rigorous maintenance schedule which meets the security standards of ISO 27001

Tribepad have independent penetration testing quarterly and some of Tribepad's customers also do their own penetration testing against the platform

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

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Tribepad complies with a recognised standard (ISO 27001)

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

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 Tribepad 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 Tribepad'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 school will be asking for personal data from individuals to enable the school to verify the candidate has permission to work in the UK, are cleared to work and to verify their identity to be able to offer employment. The school will also be checking suitability through securing references and medical clearances for the role we are recruiting them for.
The school will be relying on the following lawful bases and special category processing conditions:

Lawful bases- the school's lawful bases for processing personal information are:

- UK GDPR Article 6(1)(b) - for the performance of a contract. In addition, the school relies on the processing condition at Schedule 1, part 1, paragraph 1 of the Data Protection Act 2018, i.e. the processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on us or on prospective/current employees.

- UK GDPR Article 6(1)(c) – enables the school to comply with its legal obligations as an employer. Where an individual provides the school with any information about reasonable adjustments, they may require under the Equality Act 2010 the lawful basis the school rely on for processing this information is UK GDPR Article 6(1)(c), to comply with its legal obligations under the Act.

- UK GDPR Article 6(1)(e) - for the performance of the school's public task or in the exercise of official authority. In addition, the school rely on the processing condition at Schedule 1, part 2, paragraph 6(2)(a) of the Data Protection Act 2018 i.e. this applies to carrying out Disclosure Barring Service checks.

- UK GDPR Article 6(1)(f) - for the purposes of a school's legitimate interest (the school can use 'legitimate interests' if it can demonstrate that the processing is for purposes other than for performing its tasks as a public authority). In this context, this means compliance with school policies etc, premises security, school IT systems, audit trails, employee CCTV, lone working systems etc.

and

The lawful basis the school rely on to process any information they provide which is special category data, such as information about a candidates race or ethnicity, religious beliefs, sexual orientation, political opinions, trade union membership, information about their health, including any medical condition, health and sickness records, is UK GDPR Article 9(2)(b), which relates to the schools obligations in employment and the safeguarding of their fundamental right and Schedule 1, Part 1(1) of the DPA2018 which again relates to processing for employment purposes.

The school process information about criminal convictions and offences. The lawful basis the school rely on to process this data is UK GDPR Article 6(1)(e) for the performance of its public task. In addition, the school rely on the processing condition at Schedule 1, Part 2, paragraph 6(2)(a) of the UK Data Protection Act 2018. The school may only use information relating to criminal convictions where the law allows them to do so. This will usually be where such processing is necessary to act in accordance with our regulatory and other legal obligations. Although this will be rare, the school may also use information relating to criminal convictions where it is necessary in relation to legal claims.

The lawful basis for processing personal data is contained in the school's Privacy Notice (Workforce).

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	Significant	High
Asset protection and resilience	Possible	Significant	High
Data Breaches	Possible	Significant	Medium
Subject Access Request	Possible	Significant	Medium
Data Retention	Remote	Significant	Medium
Data Loss	Possible	Significant	High
Failure to have "back-out" plan in place if provider contract ends or provider goes into liquidation	Possible	Severe	High

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 or high	Yes/No
Data transfer; data could be compromised	Security protocols in place, end to end encryption, encryption at rest	Reduced	Low	
Asset protection and resilience	Business Continuity in place. Backup servers insitu	Reduced	Low	
Data Breaches	Reported by Tribepad. Systems in place	Reduced	Low	
Subject Access Request	Procedures in place to deal with rights of access to personal data	Reduced	Low	
Data Retention	School's data retention policy adhered to	Reduced	Low	
Data Loss	Business Continuity in place. Backup servers insitu	Reduced	Low	
"back-out" plan in place if provider contract ends	Contractual obligations	Reduced	Low	

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Vicki Poole	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Vicki Poole	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: N/A If overruled, you must explain your reasons		
Comments:		
Consultation responses reviewed by: If your decision departs from individuals' views, you must explain your reasons		
Comments:		
This DPIA will kept under review by:	Vicki Poole	The DPO should also review ongoing compliance with DPIA