Data Protection Impact Assessment (People Information and Management Systems (PIMS))

Summerhill School accesses PIMS (MidlandHR) which sits on a private network. 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 PIMS (MidlandHR) sits on a private network 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 PIMS (MidlandHR) 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 private network is important to determine applicable law. The school will need to satisfy its responsibilities in determining whether the security measures the private network provider has taken are sufficient, and that the rights of the data subject under the 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.

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. PIMS has two interfaces: (1) MyHR – which provides access via a dedicated login for all employees to a personal dashboard interface; (2) PIMS – which provides access to managers via a dedicated login for managers to manage their employees. It also assists with the management of payroll, pensions and other back end issues. PIMS will improve accessibility and ensure information security when working within the school and remotely. Summerhill 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 PIMS the school aims to achieve the following: 1. Scalability 2. Reliability 3. Resilience 4. Delivery at a potentially lower cost by reducing inefficiencies 5. Reduce HR administration by devolving responsibilities through self service 6. Improve data accuracy by making employees responsible for their information 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

Information relating to workforce related issues is visible via the MyHR dashboard for personnel, and PIMS dashboard for managers. The former has the functionality to capture personal details, manage absence, pay and benefits, employment, career and development. The latter has the functionality to approval of holidays, contract changes, sickness notes, etc. These files can then be accessed from any location via a web browser using SSL encryption.

PIMS sits on the Dudley MBC network (private intranet).

MidlandHR cannot do anything with the school's data unless they have been specifically instructed by the school. The schools Privacy Notice will be updated especially with reference to the storing of payroll, pensions and personnel data in PIMS.

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) and (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 PIMS and in paper based files. The information is retained according to the school's Data Retention Policy. PIMS has an inbuilt data retention module which, on behalf of schools, will delete workforce records once retention for leavers exceeds + 6 years. This meets the requirements of data minimization. However, some of the information relating to leavers is retained for pension purposes.

What is the source of the data? – Information held on PIMS is obtained from identity documents such as an employee's drivers licence, passports and proof of address documents *(these are flagged on PIMS),* forms completed at the start of employment, correspondence, interviews, meetings, qualifications and assessments *(these are flagged on PIMS)*. In some cases Summerhill School personal data may be obtained from third parties, such as references from former employers, information from background check providers *(these are flagged on PIMS),* information from credit reference agencies and information from criminal record checks permitted by law. The aforementioned documents are not uploaded into PIMS but may be included in the school's workforce files which are held, securely with limited access, as a hard copy.

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 (within Dudley MBC's ICT network). Storage of personal and 'special category' data in PIMS.

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? – Workforce data relates to personal 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, bank details, national insurance number, marital status, next of kin, dependents and emergency contacts. Special categories of data (such as gender, age, ethnic group). Contract information *(such as start dates, terms and conditions of employment, hours worked, post, roles and salary information, pensions, nationality and entitlement to work in the UK)*. Along with salary information any additional payments, i.e. TLR, is included. PIMS also capture information on work shift patterns. Work absence information including details of periods of leave taken by the employee, including holiday, sickness absence, family leave, maternity leave, and sabbaticals, and the reasons for the leave. Information about medical or health conditions, including whether or not the employee has a disability, details of trade union membership and equal opportunities monitoring information. **Special Category data?** – Some of the personal data collected falls under the 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 all of the school's workforce. Additionally, personal data is also held respecting the school's workforce, Board of Governors, Volunteers, and Contractors. **How long will you keep the data for?** – Workforce data will be kept in line with the schools' data retention policy as follows (termination of employment + 6 years). However, some of the information relating to leavers is retained for pension purposes.

Scope of data obtained? – How many individuals are affected? 1100 And what is the geographical area covered? Workforce 93 Board of Governors 15 and Volunteers 10.
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? – Summerhill School collects and processes personal data relating to its employees when entering into an employment contract and to meet its obligations under an employee's employment contract. Summerhill School needs to process personal data to administer payroll, benefits, local authority pensions scheme, teachers pensions scheme, and tax and national insurance entitlements. Through the Privacy Notice (Workforce) and (Governors and Volunteers) 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 the personal files will be controlled by username and password. MidlandHR is hosting the data and has the ability to access data on instruction of Summerhill School who is the data controller for the provision of supporting the service as stated in MidlandHR Terms and Conditions. New inductees are given a unique log in to set up their own MyHR account. This is then assigned to the reporting manager (PIMS). A new inductee has sight of the MyHR Privacy Notice and this has to be accepted before the new employee can proceed to create their own individual account. The school will be able to upload personal data from its PC for the data to be stored in PIMS via a secure private network. **Do they include children or other vulnerable groups?** – No

Are there prior concerns over this type of processing or security flaws? – PIMS sits on the Dudley MBC network (private intranet). Access is via SSL encryption.

Summerhill 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: Data and functionality access is assigned according to user definable security profiles. Once the user has successfully logged on with their password authenticated, they will be granted access according to the security profile in which they reside. Access to data may be controlled at functional, screen, and field level. Access to list content can be restricted with access defined as, fully editable, read-only, non-visible. When accessing support channels, user accounts are created on MHR's Service cloud portal

- **ISSUE**: Transfer of data between the school and the cloud
  RISK: Risk of compromise and unlawful access when personal data is transferred.
  MITIGATING ACTION: The use of Secure File Transfer Protocol (SFTP) to enable the secure transfer of files. iTrent database encryption at rest. TLS, secure transfer of e-mail between the customers e-mail server and MidlandHR e-mail server. Encryption at rest

- **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage.
  MITIGATING ACTION: MidlandHR provides an SFTP service for transferring of data between customers and MidlandHR. Data on the SFTP server is encrypted at rest and in transit. TLS for e-mail encryption is available as an additional service. Alternatively MidlandHR offer a secure mail service whereby users when required login to the secure mail service portal to access e-mails

- **ISSUE:** Disaster recovery
  RISK: GDPR non-compliance
  MITIGATING ACTION: MidlandHR have in place a Business Continuity Plan designed to ensure that MidlandHR continues all functions in the event of a disaster. This plan is reviewed twice yearly and is dynamically updated as the organisation changes. MidlandHR has been certified to ISO27001 since 2005 and are currently following the ISO22301 guidelines to ensure MHR maintain a structured approach to the business

- **ISSUE:** System back up
  RISK: GDPR non-compliance
  MITIGATING ACTION: Full database backups are performed daily. All data backups shall remain within the United Kingdom used for hosting. Escrow data backup undertaken

- **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 PIMS are located within the UK

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: GDPR non-compliance
  MITIGATING ACTION: PIMS has the functionality to provide rights of individuals management of information access where the data subject has restricted disclosure or withdrawn consent. Additionally, MidlandHR has a two factor authentication process which limits access to the Back Office of PIMS via registered IP addresses. Access to iTrent is controlled via user name and password authentication

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: GDPR non-compliance
  MITIGATING ACTION: The system has data retention functionality. Authorised users can apply data retention schedules to individuals or groups of individuals and this retention period can be applied to leavers and also applicants. The system comes with a minimum retention period set (leaver date + 6 years) however authorised users can override the stated period with their own retention periods in line with their data retention policy, allowing for overrides when there is a justified reason for keeping the data longer for the school; i.e. some of the information relating to leavers is retained for pension purposes

- **ISSUE:** Responding to a data breach
  RISK: GDPR non-compliance
  MITIGATING ACTION: Users of PIMS can report incidents via the Customer Portal 24/7, or via telephone 9am - 5pm UK time (Monday to Friday excluding bank holidays). Through a dedicated support line customers are able to contact the service desk whereupon each call is given a unique reference number. The call is assigned to the appropriate member of the support team and tracked at all times by the service desk

- **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: PIMS has the functionality to handle and respond to Subject Access Requests. PIMS has a core form for data access requests that allows the user to elect the employee and the type of data. A data access report will present all data in relation to the individual

- **ISSUE:** Data Ownership
  RISK: GDPR non-compliance
  MITIGATING ACTION: The school remains the data controller. iTrent is the data processor and Summerhill School and MidlandHR is the data processor. Please see Terms and Conditions

- **ISSUE:** No deal Brexit
  RISK: GDPR non-compliance
  MITIGATING ACTION: The solution is currently hosted in 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: Information is hosted on MidlandHR's data centres, provided as a dedicated application server from a dedicated database. The hosted service is not multi tenanted as either Application or Database tiers. This ensures that all customers are segregated to high standards and the service remains at optimum level

  At both sites (primary and back up) there is restricted physical access, ID/Swipe cards for staff and CCTV. Both sites have visitor access control procedures and are manned 24/07/365. The firewall at the MidlandHR data centre has specific access controls for each customer

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

- **ISSUE:** Security of Privacy
  RISK: GDPR non-compliance
  MITIGATING ACTION: Infrastructure within MidlandHR's datacentres are regularly scanned using QualysGuard. Authenticated scans are performed to identify vulnerabilities. This data is supplemented by threat intelligence form NCSC, CERT and security industry bodies to feed vulnerability/patch management processes. The infrastructure is patched as required. Systems are regularly scanned by our Qualys suite to ensure all devices are at the required patch levels MHR perform an annual CREST penetration test of the software, hosted service and corporate network

  Conforms to a recognised standard, for example, CSA CCM v3.0 or ISO/IEC 27035:2011 or SSAE-16 / ISAE 3402. It has Cyber Essentials as a security governance standard

  MidlandHR is ISO 27001 and ISO 9001 certified. MidlandHR is registered with the ICO and Lloyds Register LRQA

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 PIMS 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 (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 EU, Certified, Penetration Testing and Audit	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:	Martyn Palfreyman	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Martyn Palfreyman	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 provided]**		
DPO advice accepted or overruled by:	**[Yes/No]**	If overruled, you must explain your reasons
Comments: **[DPO Advice provided]**		
Consultation responses reviewed by:	**[Insert name]**	If your decision departs from individuals' views, you must explain your reasons
Comments: **[Comments provided]**		
This DPIA will kept under review by:	Vicki Poole	The DPO should also review ongoing compliance with DPIA