

**Data Protection Impact Assessment (SIMS)**

*As a Christian school our vision is to promote ‘Life in All its Fullness.’ Our ethos is based on our 12 Christian values of hope, honesty, patience, joy, forgiveness, tolerance, thankfulness, respect, kindness, friendship, gentleness and love. It is within the vision and the ethos that this policy is written and will be implemented.*

Date issued: January 2021

Review date: January 2022



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.    Holly Hill Schoolwill 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 local database solution the school aims to achieve the following:     1. Safeguarding data 2. Security 3. Reliability 4. Resilience 5. Delivery at a potentially lower cost 6. Link2ICT backup data 7. Update of documents in real time |

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 Notices (student and workforce) for the school provides the legitimate basis of why the school collects data.    **How will you collect, use, store and delete data?** – The information collected by the school is retained on the school’s computer systems and in paper files. The information is retained according to the school’s Records Management Policy.    **What is the source of the data? –** Information held on SIMS is limited to pupil and staff (including long term agency workers).  Student information is collected via admission forms when students join the school, updates from parents (eg due to house move), Common Transfer File (CTF) from previous schools. Student information also includes assessments, attendance, consents to share photos, etc.  Workforce information is collected through application forms; details from agency, information obtained from identity documents, forms completed at the start of employment, correspondence, interviews, meetings and assessments.    **Will you be sharing data with anyone?** – Holly Hill School routinely shares student information with relevant staff within the school, schools that the student attends after leaving, the Local Authority, the Department for Education, Health Services, Learning Support Services, Capita SIMS and various safeguarding services. The data is also used for the termly census to the Local authority.    Holly Hill Schoolroutinely shares workforce information internally with people responsible for HR and recruitment (including payroll), senior staff, with the Local Authority, and the Department for Education. Personnel information is also shared with the SIMs FMS financial management system to assist with budgeting.  **What types of processing identified as likely high risk are involved?** – Current version of SIMS does not store this data in the cloud. Information is held securely on servers in school. Back up of servers take place using hardware encryption via Link2ICT. |
| **What is the nature of the data?** – Student data relates to personal identifiers and contacts (such as name, unique pupil number (UPN), contact details and address).  Characteristics (such as ethnicity, language, nationality, gender, religion, data of birth, country of birth, free school meal eligibility). Special education needs, safeguarding information, medical and administration (doctor’s information, child health, dental health, allergies, medication and dietary requirements). Attendance information, assessment, attainment and behavioural information. The school also obtains data on parents/guardians/carers including their name, address, telephone number and e-mail address.    Workforce data relates to personal information (such as name, employee or teacher number, national insurance number. 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). Special categories of data (such as gender, age, ethnic group, contact details), attendance, performance management, Work absence information, information about criminal records, details of any disciplinary or grievance procedures. Information about medical or health conditions, are all held on the HR Portal which is cloud based hosted by Birmingham City council under their SLA.    **Special Category data?** – Some of the personal data collected falls under the GDPR special category data. This includes race; ethic origin; religion; biometrics; and health. These may be contained in the Single Central Record, Capita SIMS, child safeguarding files, MyConcern, SEN reports, etc.    **How much data is collected and used and how often?** – Personal data is collected for all students on admission and then updated each year. Some data such as pupil progress is collected more frequently.    **How long will you keep the data for?** – The retention schedule recommended to schools by IRMS (Information and Records Management Society) says that information about students should not be retained once they leave the establishment. We forward pupil data to the next school upon leaving, and the record becomes non active. |

|  |
| --- |
| **Scope of data obtained?** –Nursery pupils (up to 60), School pupils (up to 180), workforce 35. |
| **Describe the context of the processing**  The school provides education to its students with staff delivering the National Curriculum    **What is the nature of your relationship with the individuals?** – Holly Hill Schoolcollects and processes personal data relating to its students and employees to manage the parent/student and employment relationship.    Through the Privacy Notice (student/workforce) Holly Hill Schoolis 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 files will be controlled by username and password. SIMS is stored on our own internal server which is in a secured room.    **Do they include children or other vulnerable groups?** – Some of the data may include special category data such as child safeguarding records, SEN records, free school meal eligibility.    **Are there prior concerns over this type of processing or security flaws? –** Current version of SIMS does not store this data in the cloud. Back up of servers take place using hardware encryption Link2ICT secure access. |

|  |
| --- |
| Holly Hill Schoolrecognises a number of General Data Protection Regulations issues as follows:     * **ISSUE:** Responding to a data breach   **RISK:** GDPR non-compliance  **MITIGATING ACTION:** SIMS Capita is an ICO registered company, fully compliant with GDPR data security handling and reporting     * **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:** SIMS has the functionality within the reports menu to handle and respond to Subject Access Requests     * **ISSUE:** GDPR Training   **RISK:** GDPR non-compliance  **MITIGATING ACTION:** Appropriate training is undertaken by personnel that have access to SIMS     * **ISSUE:** Security of Privacy   **RISK:** GDPR non-compliance  **MITIGATING ACTION:** SIMS is ISO 27001 certified     * **ISSUE:** 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   **RISK:** The school is unable to exercise the rights of the individual  **MITIGATING ACTION:** SIMS provides the technical capability to ensure the school can comply with such requests. |
| **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 processing of this data will allow the school to function safely. We know where our students are at any time and can access the vital information we need to keep them safe. We can build up patterns of academic achievement and attitude so that we can best support our students and their families.    Combined staff and student data allows for school organisation with registers, to ensure correct attendance records, to allow swift response if a child is not in school and school has not been notified. |

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? |
| As the system is already in use there is no need to consult stakeholders.    Should systems change we would consult more stakeholders. |

Step 4: Assess necessity and proportionality

Step 4: Compliance and risks

|  |
| --- |
| **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 (Student and Workforce). The Legitimate basis includes the following:     * Childcare Act 2006 (Section 40 (2)(a) * The Education Reform Act 1988 * Further and Higher Education Act 1992, * Education Act 1994; 1998; 2002; 2005; 2011 * Health and Safety at Work Act * Safeguarding Vulnerable Groups Act * Working together to Safeguard Children Guidelines (DfE)       The school has a Subject Access Request procedure in place to ensure compliance with Data Protection Law    The cloud based solution will enable the school to uphold the rights of the data subject? The right to be informed; the right of access; the right of rectification; the right to erasure; the right to restrict processing; the right to data portability; the right to object; and the right not to be subject to automated decision-making    The school will continue to be compliant with its Data Protection Policy |

Step 5: Identify and assess risks

|  |  |  |  |
| --- | --- | --- | --- |
| **Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risksas necessary. | **Likelihood of harm** Remote, possible or probable | **Severity of harm** Minimal, significant or severe | **Overall risk**  Low, medium  or high |
| * Data transfer to another school; data could be compromised * Asset protection and resilience * Data Breaches * Subject Access Request * Data Retention | Possible    Possible  Possible  Possible  Possible | Severe    Significant  Significant  Significant  Significant | Medium    Medium  Medium  Medium  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**  Eliminated reduced accepted | **Residual risk**  Low medium high | **Measure approved** Yes/no |
| Data Transfer      Asset protection & resilience    Data Breaches      Subject  Access  Request    Data  Retention | Secure network, end to end encryption    Data Centre in EU, Certified,  Penetration Testing and Audit    Documented in contract with Link2ICT and owned by school  Technical capability to satisfy data subject access request    Implementing school data retention periods in the cloud | Reduced    Reduced      Reduced    Reduced      Reduced | Medium    Medium      Low    Low      Low | Yes    Yes      Yes    Yes      Yes |

Step 7: Sign off and record outcomes

|  |  |  |
| --- | --- | --- |
| This DPIA will kept under review by: | Jo Robinson  DPO | The DPO should also review ongoing compliance with DPIA |