# MODEL DPIA FOR SCHOOLS

This template is an example of how you can record your Data Protection Impact Assessment (DPIA) process and outcome. It follows the process set out in the ICO’s DPIA guidance.

You may find this example useful when completing your own DPIAs but as Medical Tracker is not the Data Controller, responsibility for completing DPIA’s must rest with Schools.

Sections relating to approval and consultation have not been fully completed as these are internal matters for the school. Examples given such as retention periods, lawful basis, and internal security measures for schools are not to be incorporated into your own DPIA without verifying the applicability of those examples for your scenarios.

# COMPANY INFORMATION

Name: Conkaa Limited (Medical Tracker)

Address: 24, 25 & 25A Cornmarket, Penrith, Cumbria, CA11 7HS

Phone: 020 3868 0776

Website: [www.medicaltracker.co.uk](http://www.medicaltracker.co.uk)

Company Registration: 10253269

ICO: ZA509399

ISO27001: 398492022

DPO: Katie Venditti

DPO e-mail: [katie@medicaltracker.co.uk](mailto:katie@medicaltracker.co.uk)

Sales e-mail: [sales@medicaltracker.co.uk](mailto:sales@medicaltracker.co.uk)

Support e-mail: [support@medicaltracker.co.uk](mailto:support@medicaltracker.co.uk)

# 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. |
| The project is the deployment of Conkaa’s Medical Tracker platform to record, track, and manage student, staff and visitor health.  The project will necessarily require the processing of special categories of data (health including disability) including that regarding persons under the age of 18. As the processing is more than occasional or incidental, the completion of a DPIA is required in order to ensure data protection by design and by default, that risks are assessed and managed, and that the processing is lawful, fair, and transparent. |

# 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 processing involves the collation of student, staff, visitor and parent/carer data by the school. Medical Tracker links to the school MIS through an intermediary company (usually Wonde or Xporter). Data is then pulled through regularly to ensure the information is current. As the data collected is generated through the school’s MIS or manual input the data was originally obtained through parents and guardians of students, the students themselves, and from other professionals. As the data is owned by the school, the school will decide who to share the data with, this might include various stakeholders. The school uses the Medical Tracker platform to process data that is already collected and processed.  A list of sub-processors is available on the Medical Tracker website. Please note that not all the sub-processors listed are relevant to schools. All sub-processors have been thoroughly vetted and follow the highest security protocols as well as being subject to Non-Disclosure Agreements. Sub-processors retain the data in line with the Medical Tracker Back Up Policy which is available on the website. All data is encrypted in transit and at rest using industry standards and best practice.  As the controller, the school has control over the data and deleting the data in line with the school’s retention schedule. Data deleted from the Medical Tracker platform will be stored by Medical Tracker for 30 days after deletion in line with the Medical Tracker Back Up Policy.  If the school decides to terminate the contract then the information held in Medical Tracker should be downloaded within 90 days. After that the information will be purged from all Medical Tracker servers and systems.  All data is stored on servers in the UK. Information security is central to Medical Tracker’s processes and they have achieved an international standard in this - the ISO 27001 certification. All staff undergo regular training and are DBS checked. |

|  |
| --- |
| **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? |
| The data includes:  Staff   * Staff ID * Staff email * Title * Legal forename * Legal last name * Staff role * Medical qualifications (e.g. First Aid at Work) – start date and end date * Details of medical conditions (optional) * Name of GP and address of surgery (optional)   Students   * Name * DOB * Current NC Year/Class * UPN * Gender * Emergency contacts * Parent/Guardian * Address * Medical needs * Medical conditions * GP details * Care plans * Medication * Demographics (optional - PP/LAC etc.)   (If the student has been involved in an accident their personal data will be recorded next to the incident they were involved in).  Parents/Guardians   * Parent name * Parent email * Parent mobile * Address * Relationship to pupils (mother/father etc)   Visitors  If a visitor is injured the following data is recorded:   * Name * Email address * Address * Gender * Company * Date of birth * Telephone number * Details of incident   The data will be retained until either 6 years have elapsed commencing the start of the financial year following the incident or when the student turns 25, whichever falls later. *– This is an example; the school will need to determine and document the appropriate retention periods for the data.*  The data will be stored electronically on a system provided by Medical Tracker under the instruction of the 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)? |
| The school has a direct relationship with all parties mentioned in the data with the exception of named healthcare providers. Due to the nature of this relationship, there will be a perceived imbalance of power between the school and the data subjects.  Data concerning children is an essential part of the process. The underlying processing is essential for complying with Department for Education standards and would occur without this project. The project will enable more controlled access to the data, ensure that those who need it have access in a more timely fashion, and provide direct oversight to the parents and guardians.  Due to the essential nature of the processing, data subjects will have limited control over the processing. In certain scenarios, the school may afford an opt-out for parents and guardians of students. In those events, the data will still be processed but in a more manual fashion.  The project relies on technology of a high level of maturity which is both specialised for and well established for this task. Security features include role-based access, user authentication, ability to revoke access at any time, usage auditing, and encryption among other measures. Specific security considerations are addressed in the Step 6 of this DPIA. |

|  |
| --- |
| **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 purpose of the deployment of Medical Tracker is to enable the school to record, track and manage student, staff and visitor health.  The data captured can offer insight into accident hotspots. It keeps parents and carers up to date, and ensures relevant parties are kept up to date about the health of students. Immediate access is available for life saving situations. A full history of all medical information is available for specific stakeholders. The standardised recording of information ensures legal and statutory duties are met.  Medical Tracker stores the data the school already stores and utilises (either using paper records or in spreadsheets). It offers a safer, reliable and efficient process.  Department for Education guidelines state this information must be kept and that protocol around notifying parents must be followed, therefore the ‘risk’ is far outweighed by the benefit of adhering to DfE safeguarding guidelines. |

# 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 processing is necessary for the fulfilment of a public task, consultation of data subjects, parents, and guardians is not warranted. Security and data protection professionals have been consulted in relation to the specific tools being deployed to achieve the stated objectives. Their responses will be set out in Step 7 of this DPIA. |

# 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? |
| *Decisions regarding Article Lawful Basis, Article 9 Conditions, and Schedule 1 Conditions are those of the controller (school). The section below includes examples that may be available to the school depending on the specific uses of the data and personnel involved.*  The lawful basis for processing under GDPR shall be Article 6 (1) (e) ‘Public Task’ for the reason that the requirement to process such data for these purposes is set out in Department for Education Safeguarding Guidelines and Health and Safety Legislation and that the processing is taking place in delivery of a core operation of a public service.  The lawful conditions for processing special categories of data shall be Article 9 (2) (b) ‘Employment and Social Security’ on the basis of providing for the social protection of the students, Article 9 (2) (g) ‘Substantial Public Interest’ on the basis of the fulfilment of obligations set out in public guidance and legislation. Under the Data Protection Act, the conditions for special categories of data shall be those of Schedule 1, Part 1 ‘Employment, Social Security, and Social Protection’, and Part 2 Substantial Public Interest Provisions of ‘Safeguarding of Children and Individuals at Risk’, and ‘Insurance’.  The processing will achieve the stated purposes without unduly exceeding them. Access to data is restricted and control measures in place to prevent the reuse for new purposes which are not consistent with the existing purposes.  The structured nature of the platform makes compliance with data subject rights more practicable and thus these are facilitated in a way which was not possible with manual and disparate records. |

# 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. These are inherent risks before any measures are put into effect to reduce these. | Likelihood of harm | Severity of harm | Overall risk |
|  | Remote, possible or probable | Minimal, significant or severe | Low, medium or high |
| R01 – Loss of data integrity - accidental | Probable | Significant | High |
| R02 – Loss of confidentiality – accidental | Possible | Severe | High |
| R03 – Loss of availability – accidental | Probable | Significant | High |
| R04 – Loss of data integrity – malicious – external threat | Probable | Significant | High |
| R05 – Loss of confidentiality – malicious – external threat | Probable | Severe | High |
| R06 – Loss of availability – malicious – external threat | Probable | Significant | High |
| R07 – Loss of data integrity – malicious – school internal threat | Possible | Significant | Medium |
| R08 – Loss of confidentiality – malicious – school internal threat | Possible | Severe | High |
| R09 – Loss of availability – malicious – school internal threat | Possible | Significant | Medium |
| R10 – Loss of data integrity – malicious – supplier internal threat | Possible | Significant | Medium |
| R11 – Loss of confidentiality – malicious – supplier internal threat | Possible | Severe | High |
| R12 - Loss of availability - malicious - supplier internal threat | Possible | Significant | Medium |
| R13 – Inappropriate reuse of data – supplier | Possible | Minimal | Medium |
| R14 – Inappropriate reuse of data – school | Possible | Minimal | Medium |
| R15 – Inappropriate data access by a foreign power | Possible | Minimal | Medium |
| R16 – Inappropriate data access by the state | Possible | Minimal | Medium |
| R17 – Data accessed by a data subject leading to harm | Possible | Severe | High |
| R18 – Noncompliance with data subject rights | Probable | Significant | High |
| R19 – Noncompliance with other legal and regulatory requirements | Probable | Significant | High |
| R20 – Data retained in excess of retention periods | Probable | Minimal | 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** |
|  |  | **Steps Taken by Medical Tracker to protect Data** | **Eliminated reduced accepted** | **Low medium high** | **Yes/ no** |
| R01, R02, R03, R04, R05, R06, R10, R11, R12, R13, R15, R16, R17 |  | Physical Access Controls: Data Processor shall take reasonable measures to prevent physical access, such as security personnel and secured buildings and factory premises, to prevent unauthorised persons from gaining access to Personal Data, or ensure Third Parties operating data centres on its behalf are adhering to such controls. | Reduced | Low |  |
| R01, R02, R03, R04, R05, R06, R07, R08, R09, R10, R11, R12, R13, R14, R15, R16, R17 |  | System Access Controls: Data Processor shall take reasonable measures to prevent Personal Data from being used without authorisation. These controls shall vary based on the nature of the Processing undertaken and may include, among other controls: authentication via passwords; two-factor authentication; documented authorisation processes; documented change management processes; and/or, logging of access on several levels. | Reduced | Low |  |
| R01, R02, R03, R04, R05, R06, R07, R08, R09, R10, R11, R12, R13, R14, R15, R16, R17 |  | Data Access Controls: Data Processor shall take reasonable measures to provide that: Personal Data is accessible and manageable only by properly authorised staff; direct database query access is restricted; application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the Personal Data to which they have privilege of access; and, that Personal Data cannot be read, copied, modified or removed without authorisation in the course of Processing. | Reduced | Low |  |
| R01, R02, R03, R04, R05, R06, R07, R08, R09, R10, R11, R12, R13, R14, R15, R16, R17 |  | Transmission Controls: Data Processor shall take reasonable measures to ensure that it is possible to check and establish to which entities the transfer of Personal Data by means of data transmission facilities is envisaged so Data cannot be read, copied, modified or removed without authorisation during electronic transmission or transport. | Reduced | Low |  |
| R01, R03, R04, R06, R07, R09, R10, R12 |  | Input Controls: Data Processor shall take reasonable measures to provide that it is possible to check and establish whether and by whom Data has been entered into, modified or removed from data processing systems. Data Processor shall take reasonable measures to ensure that (i) the Personal Data source is under the control of the Customer; and (ii) Personal Data integrated into the Service is managed by secured transmission from the Customer. | Reduced | Low |  |
| R01, R03, R04, R06, R07, R09, R10, R12 |  | Data Backup: Back-ups of the databases in the Service are taken on a regular basis, are secured, and encrypted to ensure that Personal Data is protected against accidental destruction or loss when hosted by Data Processor. | Reduced | Low |  |
| R01, R02, R03, R04, R05, R06, R07, R08, R09, R10, R11, R12, R13, R14, R15, R16, R17 |  | Data Security: Where appropriate and reasonable, Data Processor should make use of accepted Data Security controls including but not limited to encryption, pseudonymisation and anonymisation. | Reduced | Low |  |
| R01, R02, R03, R04, R05, R06, R07, R08, R09, R10, R11, R12, R13, R14, R15, R16, R17 |  | Logical Separation: Data from different Data Processor’s Customers is logically segregated on Data Processor’s systems to ensure that Personal Data that is collected for different purposes may be Processed separately. | Reduced | Low |  |
| R01, R02, R03, R04, R05, R06, R07, R08, R09, R10, R11, R12, R13, R14, R15, R16, R17 |  | Network Security Controls: Data Processor shall implement appropriate network security controls based on risk assessment as it relates to Data Protection; commonly including Firewalls, Anti-Malware and system logging. | Reduced | Low |  |
| R01, R02, R03, R04, R05, R06, R07, R08, R09, R10, R11, R12, R13, R14, R15, R16, R17 |  | Security Testing and Assurance: Data processor shall establish mechanisms for testing and assessing the effectiveness of technical or organisational measures used for establishing data security. | Reduced | Low |  |
|  |  | **Steps to be taken By the School to Protect the Data** | **Eliminated reduced accepted** | **Low medium high** | **Yes/ no** |
| R04, R05, R06, R07, R08, R09, R14, R17 |  | There is a risk that a staff member leaves a computer on and unattended so others accidentally get access, however within the platform you can switch on a 20 minute ‘time out’, whereby after a period of inactivity Medical Tracker is logged out of automatically. | Reduced | Low |  |
| R04, R05, R06, R07, R08, R09, R14, R17 |  | The school itself would be responsible for communicating the importance of logging out of the platform or not leaving it unattended when not in use. | Reduced | Low |  |
| R04, R05, R06, R07, R08, R09, R14, R17 |  | The school MIS stores personally identifiable information about students, parents and staff. Wonde/Xplorer provides a read-only API feed to draw the data from the school MIS into Medical Tracker. Wonde/Xplorer do not use or view this information, their sole purpose is to transfer data into Medical Tracker. | Reduced | Low |  |
| R04, R05, R06, R07, R08, R09, R14, R17 |  | Ensuring strict access controls are in place and strong passcodes are required. | Reduced | Low |  |
| R01, R02, R03, R04, R05, R06, R07, R08, R09, R14, R17 |  | Ensuring safeguarding protocols are communicated to all users. | Reduced | Low |  |
| R01, R02, R03, R04, R05, R06, R07, R08, R09, R14, R17 |  | Regular security reviews. | Reduced | Low |  |
| R01, R02, R03, R04, R05, R06, R07, R08, R09, R14, R17, R18, R19, R20 |  | Training for staff. | Reduced | Low |  |
| R01, R02, R03, R04, R05, R06, R07, R08, R09, R14, R17, R18, R19, R20 |  | Writing internal guidance or processes to avoid risks (school policy). | Reduced | Low |  |
| R01, R03, R14, R17, R18, R19, R20 |  | Reviewing retention periods. | Reduced | Low |  |
| R13, R14, R18, R19 |  | Reducing the scope of the processing. | Reduced | Low |  |
| R13, R15, R16, R18, R19, R20 |  | Ensuring a clear data sharing agreement is in place. | Reduced | Low |  |
| R18, R19 |  | Making changes to the privacy notices. | Reduced | Low |  |

# STEP 7: SIGN OFF AND RECORD OUTCOMES

|  |  |  |
| --- | --- | --- |
| **Item** | **Name/position/date** | **Notes** |
| **Measures approved by:** |  | Integrate actions back into project plan, with date and responsibility for completion |
| **Residual risks approved by:** |  | If accepting any residual high risk, consult the ICO before going ahead |
| **DPO advice provided:** |  | DPO should advise on compliance, step 6 measures and whether processing can proceed |
| Summary of DPO advice: | | |
| **DPO advice accepted or overruled by:** |  | 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:** |  | The DPO should also review ongoing compliance with DPIA |