Data Protection Impact Assessment (Medical Tracker)

Brook Primary School operates a cloud based system. As such Brook 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.

Brook Primary School recognises that moving to a cloud service provider has a number of implications. Brook 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 a cloud- based system 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 cloud is important to determine applicable law. The school will need to satisfy its responsibilities in determining whether the security measures the cloud provider has taken are sufficient, and that the rights of the data subject under the UK GDPR is satisfied by the school.

Brook 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. The cloud based system will improve accessibility and ensure information security when working remotely.

Brook Primary 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 an internal server based solution the school aims to achieve the following:

1. Scalability
2. Reliability
3. Resilience
4. Delivery at a potentially lower cost
5. Supports mobile access to data securely
6. Update of documents in real time
7. Good working practice, i.e. secure access to sensitive files

Medical Tracker is an online software application to report first aid incidents, track medications and student care plans. The online forms are built to comply with Department for Education (DfE), OFSTED and RIDDOR guidelines. Medical Tracker allows Brook Primary School to comply with DfE Guidelines to accurately store records, notify parents of incidents and report serious incidents and near misses.

The cloud service provider cannot do anything with the school's data unless they have been instructed by the school. The schools Privacy Notice will be updated especially with reference to the storing of pupil and workforce data in the cloud.

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 (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 Brook Primary School Privacy Notice (Pupil) and where appropriate in Privacy Notice (Workforce).

How will you collect, use, store and delete data? – The information collected by the school is retained on Medical Tracker.

Some of the personal data collected falls under the UK GDPR special category data. This includes information relating to medical conditions, medication needed and care plans. If the student has been involved in an incident their personal data will be recorded next to the incident they were involved in. This will also include parent: name, email, address and telephone number against the student.

In terms of an incident personal data may also relate to staff/teachers: and their name, date of birth, email, home address and telephone number, and details of any medical conditions

If a visitor is injured their name, email, date of birth, telephone number and incident may also be recorded.

The information is retained in accordance with the school's Data Retention Policy.

What is the source of the data? – Routinely pupil information is collected via registration forms when pupils join the school, pupil update forms the school issue at the start of the year, Common Transfer File (CTF) or secure file transfer from previous schools. Pupil information also includes classroom work, assessments and reports. Workforce information is collected through application forms, CVs or resumes; information obtained from identity documents, forms completed at the start of employment, correspondence, interviews, meetings and assessments.

Will you be sharing data with anyone? – Brook Primary School may share pupil, workforce and visitor information with relevant staff within the school, the Local Authority, the Department for Education, Health and Safety Executive (HSE), Health Services, and Medical Tracker.

Brook Primary School may share workforce information internally with people responsible for HR, senior staff, Health and Safety Executive (HSE), Health Services, with the Local Authority, and the Department for Education.

What types of processing identified as likely high risk are involved? – Transferring 'special category' data from the school to local authority, and to hosted servers remotely. Storage

of personal and 'special category' data. The WAN link from the school is a dedicated lease line so is not shared with other users like domestic broadband users, therefore it is protected from interception.

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? – Pupil data relates to personal identifiers and contacts (such as name, unique pupil number, 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 behavioral 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, address and contact details, 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). Work absence information, information about criminal records, details of any disciplinary or grievance procedures. Assessments of performance (such as appraisals, performance reviews, ratings, performance improvement plans and related correspondence). Information about medical or health conditions.

Special Category data? – Some of the personal data collected by Medical Tracker falls under UK GDPR special category data. This includes information relating to medical

conditions, medication needed and care plans. If the student has been involved in an incident their personal data will be recorded next to the incident they were involved in.

Special category data may also be obtained from the workforce or visitors if they have had an incident whilst at school.

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 all pupils. Additionally, personal data is also held respecting the school's workforce, Board of Governors, Volunteers, and Contractors. Data relating to sports coaches and other educational specialist is contained within the Single Central Record to ensure health and safety and safeguarding within the school.

How long will you keep the data for? – Consider the data retention period as outlined in the IRMS Information Management Toolkit for Schools and the School's Data Retention Policy.

Scope of data obtained? – How many individuals are affected (pupils, workforce, governors, and volunteers)? And what is the geographical area covered? Year 7 to Year 11 pupils 459 and workforce 67.

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? – Brook Primary School collects and processes personal data relating to its pupils and employees to manage the parent/pupil and employment relationship.

Through the Privacy Notice (pupil/workforce) Brook 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 the files will be controlled by username and password. Medical Tracker is hosting the data and has the ability to access data on instruction of Brook Primary School who is the data controller for the provision of supporting the service.

The school will be able to upload personal data from its PC via a web browser for the data to be stored remotely by a service provider. Changes made through the browser when accessing Medical Tracker may update the data stored by the school.

Do they include children or other vulnerable groups? – Medical Tracker will include the following: student name, date of birth, parent details, medical conditions, medication needed and care plans. If the student has been involved in an incident their personal data will be recorded next to the incident they were involved in.

Are there prior concerns over this type of processing or security flaws? – Medical Tracker are seeking ISO 27001 accreditation, the international standard for information security management. In addition, Medical Tracker uses Amazon Web Services (AWS) in the UK.

Brook Primary School recognises 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: All users of Medical Tracker have their own accounts. Medical Tracker servers are patched continuously to reduce security vulnerabilities

  Medical Tracker authentication service undergoes a SOC 2 Type II audit by an independent auditor annually. This audit covers the Medical Tracker product, infrastructure, and policies. The SOC 2 Type II Audit Report is available to enterprise

level customers upon request with a non-disclosure agreement (NDA) signed by a corporate officer authorized to represent the company

- **ISSUE**: Transfer of data between the school and the cloud
  RISK: Risk of compromise and unlawful access when personal data is transferred.
  MITIGATING ACTION: All network traffic is encrypted using Transport Layer Security (TLS). Encryption for data at rest is automated using encrypted storage volumes. All Medical Tracker servers are situated in secure locations

- **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: Medical Tracker database dedicated clusters are deployed in a unique Virtual Private Cloud (VPC) with dedicated firewalls. Access must be granted by an IP whitelist or VPC Peering

  Medical Tracker follow best practices, including: underpinning Medical Tracker development with a secure software development lifecycle, third-party penetration testing and code review. Continuous vulnerability assessment and automated patching. Company-wide information security training and targeted refreshers

  Medical Tracker data is cloud hosted within Amazon Web Services, the following hyperlink details security procedures - https://aws.amazon.com/security/

- **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 Medical Tracker are located within the UK, within multiple geographic locations utilizing Amazon Web Services 'Software as a Service' (SaaS)

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Access to schools' data is strictly controlled and monitored at Medical Tracker, and they employ a 'least privilege' code of practice within the organisation

  Each user's access can be customized to what level of access the school would like to have (e.g. full administration rights or read-only access). Where there is a risk that a staff member leaves a computer on and unattended so others accidentally get access, the Medical Tracker platform can switch on a 20 minute 'time out', whereby after a period of inactivity Medical Tracker is logged out of automatically

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Medical Tracker is fully compliant with UK GDPR data security retention and storage. Medical Tracker has data deletion functionality

  The data the school holds will only be kept for as long as is necessary, and in accordance with the school's Data Retention Policy. Medical Tracker enables the school to delete data when required in accordance with its Data Retention Policy

  In certain circumstances, individuals have the right to erasure. This means that the data subject has the right to request that their data be deleted or removed where there is no lawful basis for its continued storage

- **ISSUE:** Data is not backed up
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: All backups are encrypted before being stored using keys from Amazon Key Management. The keys are rotated yearly and all keys required to decrypt existing backups will be stored until no longer required

  Medical Tracker is managed by MongoDB-Atlas that also resides on Amazon Web Services. Daily backups are made and retained for 7 days. Weekly backups are made and retained for 1 month. The backups are located across 3 London UK data centres and are encrypted

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Medical Tracker is fully compliant with UK GDPR data security handling and reporting

- **ISSUE:** Data Retention
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Medical Tracker has a policy where data is retained for as long as necessary to provide the service

  Whilst the school remains a customer of Medical Tracker all of its data will be kept on an on-going basis. However, should the school cancel its subscription, Medical Tracker will keep the data for 90 days. Within those 90 days the school will have the option to export all of its data, meaning the school can still adhere to DfE guidelines for keeping student incident report data for the specified data retention period

- **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: Medical Tracker has the functionality to respond to Subject Access Requests. Medical Tracker agrees to comply with Subject Access Requests relating to the data it stores

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The school remains the data controller. Medical Tracker is the data processor

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Medical Tracker is hosted on Amazon AWS servers based in London, 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: As a service, Medical Tracker is UK GDPR compliant. The data processor remains accountable for the data within the system. For the services it manages, Medical Tracker applies its own security updates. Where security updates are applicable to the infrastructure, Amazon Web Services will manage these

- **ISSUE:** Third-party Access to Data
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Before any access is granted to the school's data held in Medical Tracker, to third-party applications, the school must give explicit authorization and review the type of data that the application is requesting. The permissions can be revoked at any time by the school

- **ISSUE:** UK GDPR Training
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Appropriate training is undertaken by personnel that have access to Medical Tracker in strict compliance with ISO 27001 and agree to abide by the Medical Tracker data sharing and confidentiality policies

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Medical Tracker has various security procedures in place which ensure the safety of the school's data. These include:

  ICO Registration: Medical Tracker are registered with the Information Commissioner's Office (ICO) for data protection, the UK's independent supervisory authority, that upholds public information rights and regulatory controls in the use of personal data by data controllers such as schools

  ISO 27001: is one of the most widely recognized, internationally accepted independent security standards. Medical Tracker are going through the early stages of accreditation for ISO 27001 so a number of areas surrounding the above are changing throughout the next 6-12 months

Medical Tracker conduct penetration testing through a third-party provider, and Medical Tracker manages compliance with security policies alongside monitoring risk assessments

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.

Combined staff and student data allows for timetable creation and school organisation with registers.

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

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 (Pupil 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 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
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
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:	Mrs M Fellows	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Mrs M Fellows	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 *(the following questions were asked of the third party by the school's Data Protection Officer)*:

1. Reference is made to back up of data in the UK. Where is the hosted service for Medical Tracker located? We use Amazon AWS servers based in London, UK.

2. What security exists in terms of Medical Tracker, e.g. application security testing, penetration testing; conduct risk assessments; and monitor compliance with security policies, etc? We are going through the early stages of our accreditation for ISO 27001 so a number of areas surrounding the above are changing throughout the next 6-12 months. We conduct penetration testing through a third-party provider, our CTO manages compliance with security policies alongside monitoring risk assessments.

3. In addition what physical security exists, e.g. are the servers equipped with industry standard firewalls, does the hosting facility provide a 24 x 7 security system, video surveillance, intrusion detection systems and locked cage areas? As we host our servers with Amazon AWS you can find more information about their physical security here: https://aws.amazon.com/compliance/data-center/controls/

4. Reference is made to the EU-US Privacy Shield which suggests that Medical Tracker may transfer data to the US. The school is aware that the European Court of Justice (ECJ) has ruled that the EU-US Privacy Shield is invalid as it fails to protect privacy and data protection rules. As part of the same ruling the ECJ decided that another data transfer mechanism, Standards Contractual Clauses, or SCCs, remain valid. To meet this obligation does Medical Tracker have Standard Contractual Clauses in place? We don't transfer data outside of the UK - all servers are based in UK.

Indeed for transfer of any data outside of the UK has Medical Tracker considered the use of Standard Contract Clauses? Medical Tracker does not transfer data outside of the UK.

Where a data breach is identified on the part of the third party what process exists to notify the school? If you decide not to notify individuals, you will still need to notify the ICO unless you can demonstrate that the breach is unlikely to result in a risk to rights and freedoms. You should also remember that the ICO has the power to compel you to inform affected individuals if we consider there is a high risk. In any event, you should document your decision-making process in line with the requirements of the accountability principle.

How does Medical Tracker ensure compliance Post Brexit? As our data is stored in London, UK we will continue to be compliant with regulations surrounding Post Brexit.

Has Medical Tracker achieved any accreditation e.g. ISO 27001, Cyber Security Essentials, etc? We are in the process of obtaining our ISO 27001 however we are at the early stages. We have two companies in the Education sector and the first company is going through this currently. Once we have achieved this we will go through the same process with Medical Tracker.

DPO advice accepted or overruled by:

Accepted

If overruled, you must explain your reasons

Comments:

DPO Advice provided

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:	Mrs M Fellows	The DPO should also review ongoing compliance with DPIA