Data Protection Impact Assessment (Sleuth)

Cloud computing is a method for delivering information technology (IT) services in which resources are retrieved from the Internet through web-based tools and applications, as opposed to a direct connection to a server at the school. Old Park School operates a cloud based system. As such Old Park 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.

Old Park School recognises that moving to a cloud service provider has a number of implications. Old Park 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. Old Park 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 3

Step 2: Describe the processing 5

Step 3: Consultation process 14

Step 4: Assess necessity and proportionality 15

Step 5: Identify and assess risks 16

Step 6: Identify measures to reduce risk 17

Step 7: Sign off and record outcomes 19

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? – *Sleuth* is a software tool for tracking student behaviour and their personal and social development. It is used a number of mainstream and special schools.

Tracking is a 3-stage process involving recording data (about incidents, events and observations) which is then analysed to produce useful information that can inform school decisions and understanding of what's going on.

Recording is the first step; many schools record a significant amount of data but staff often lack the time and tools required to analyse this to turn data into useful information.

Sleuth provides a straightforward means for schools to record, analyse and produce high quality information that is targeted for every situation/audience and is available on demand in 1-click. Most importantly, it highlights the potential opportunities for analysing the recorded data to produce a huge range of reports that can be used by different staff roles in different situations.

Sleuth provides leaders and teachers with information that is used to:

- Communicate what's going on, who is involved and how staff have responded.
- Identify individuals and groups that need support and help you plan intervention strategies.
- Monitor the impact of interventions and provision, evidencing progress and improvement.
- Assisting staff with targeted information so that they always know what's going on, are able to collaborate with colleagues and develop practice that makes a real and sustainable difference to the behaviour and personal development of every student.

Old Park 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 a cloud-based solution the school aims to achieve the following:

1. Scaleability
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

The information is held securely with regular data backed up. The network is only accessible through dedicated password linked to the school.

Cloud based systems enable the school to upload documents, photos, videos, and other files to a website to share with others or to act as a backup copy. These files can then be accessed from any location or any type of device (laptop, mobile phone, tablet, etc).

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 Old Park 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 the school's computer systems and in paper files. The information is retained according to the school's Data Retention Policy.

What is the source of the data? – 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? – Old Park School routinely shares pupil information with relevant staff within the school, schools that the pupil attends after leaving, the Local Authority, the Department for Education, Health Services, Learning Support Services, RM Integris and various third-party Information Society Services applications.

Old Park 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? – Transferring 'special category' data from the school to the cloud. Storage of personal and 'special category data in the Cloud. In terms of using *Sleuth* some personal data considered as special category under GDPR may be used.

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. Characteristics and Special education needs, medical and administration (doctor's information, child health, dental health, allergies, medication and dietary requirements). Attendance information, assessment, attainment and behavioral information.

Primary Contact Address and Telephone, Date of Birth, English as an Additional Language, Email Address, Ethnicity, Free School Meals, Gender, Year/House/Tutor group, Looked After Child, Surname, First Name and Middle Name, Primary Contact Name, Pupil Premium, Statement of SEN, Pupil Needs including Type, Start/End dates Comment, Student Code (UPN), Enrol Stage, Boarder Status, Placing Authority, Caring Authority, Date of Entry, Fee Start Date, Leaving Date, Leaving Reason, Fee End Date, Destination, Referral Stage, Enquiry Name, Enquiry Job, Enquiry Email, Enquiry Phone, Authority Enquiry Date

The school also obtains data on parents/guardians/carers including their name, address, telephone number and e-mail address. Child, and relationship to the child.

Parent Enquiry Date, General Enquiry Date, Application Received Date, Offer Made Date, Offer Accepted Date, Offer Withdrawn Date, Withdrawn Reason, Referral Notes, Allergies, Medications, Medical Notes, Doctors Surgery, and Doctors Address.

Workforce data relates to personal information such as Surname, First Name and Middle Name, email address, employment position, ethnicity and gender.

Schools can turn off many of the data areas listed below if they wish to, without affecting other areas of functionality, for example turning off Documents will not affect how Seating plans work, except that any linked student documents will not be available within the feature.

Special Category data? – Some of the personal data collected falls under the UK GDPR special category data. This includes race; ethic origin; biometrics; and health. These may be contained in the Single Central Record, Arbor, child safeguarding files, SEN reports, etc. However, in terms of using *Sleuth* special category data may be captured in terms of Behaviour (e.g. incidents, trends), Documents (e.g. reports, EHICs), Incidents (e.g. bullying, well-being concerns), and Indicators & related data (e.g. pupil premium, SEN).

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? – The school will be applying appropriate data retention periods as outlined in its Data Retention Policy and the IRMS Information Management Toolkit for Schools.

Scope of data obtained? – *Sleuth* relies on minimal personal data. The school will act as the administrator and will set up access to pupils within a classroom and individual setting. Personal data will include details of the class/year and the first and second name of the pupil.

Personal data is obtained from the school's management information system. The amount of data provided to the *Sleuth* system is under full control of the school, depending on the number of features that it decides to use.

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? – Old Park 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) Old Park School is committed to being transparent about how it collects and uses data and to meeting its data protection obligation. *Sleuth* is able to support the school's obligations under UK GDPR where a data subject wishes to exercise their rights.

How much control will they have? – Access to the pupil files will be controlled by the school.

Cloud Service provider is hosting the data and will not be accessing it.

The school will be able to upload personal data from its PC for the data to be stored remotely by a service provider. Any changes made to files are automatically copied across and immediately accessible from other devices the school may have.

Do they include children or other vulnerable groups? – Some of the data in *Sleuth* may have special category data such as Behaviour (e.g. incidents, trends), Documents (e.g. reports, EHICs), Incidents (e.g. bullying, well-being concerns), and Indicators & related data (e.g. pupil premium, SEN).

Are there prior concerns over this type of processing or security flaws? – Does the cloud provider store the information in an encrypted format? What is the method of file

transfer? For example, the most secure way to transfer is to encrypt the data before it leaves the computer. Encryption does have its limitations since the encryption key will need to be shared with others to access the data.

Old Park 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: *Sleuth* data is held on servers in physically secure datacentres with server support 24x7. The data is held encrypted at rest in both the database and file storage areas. The *Sleuth* servers are on their own private network behind a firewall.

  A school can specify an IP range or specific IP addresses to prevent access to their *Sleuth* database from unidentified PCs. This can restrict access to only the PCs within school, for example.

  Sleuth server administration can only happen from SSC offices (owners of Sleuth) through restricted IP addresses. No admin access is permitted from anywhere else. All passwords are held hashed using an individual salt, this makes it almost impossible to reverse-engineer and reveal the actual password. Memorable words are held encrypted because we need to prompt for individual characters of the word.

  School Software Company (SSC) are continually improving *Sleuth* by fixing issues and adding features. These improvements are released as new versions of *Sleuth* to which schools are automatically upgraded. SSC gradually rollout new versions to schools and monitor any affects throughout the rollout to ensure the school's *Sleuth* service is unaffected.

- **ISSUE**: Transfer of data between the school and the cloud.
  RISK: Risk of compromise and unlawful access when personal data is transferred.
  MITIGATING ACTION: *Sleuth* uses HTTPS (HTTP over SSL), a web protocol that encrypts and decrypts data to and from the web server. All *Sleuth* sessions are protected by 256-bit AES encryption – note the padlock that appears in the status bar when you are using *Sleuth*. SSL is the standard security technology for creating a secure encrypted link between a web server and a browser. Data passed between the browser

and *Sleuth* is private and secure. SSL is an industry standard used by millions of websites in the protection of their online transactions with their customers.

- **ISSUE**: Security of data whilst hosted in the cloud.
  RISK: Risk of compromise and unlawful access when personal data is at rest
  MITIGATING ACTION: *Sleuth* server administration can only happen from SSC offices (owners of Sleuth) through restricted IP addresses. No admin access is permitted from anywhere else. All passwords are held hashed using an individual salt, this makes it almost impossible to reverse-engineer and reveal the actual password. Memorable words are held encrypted because we need to prompt for individual characters of the word.

- **ISSUE:** Use of third-party sub processors?
  RISK: Non-compliance with the requirements under UK GDPR
  MITIGATING ACTION: Most school/care settings using *Sleuth* have a Management Information System (MIS) to manage the personal data they control about data subjects. A subset of this data can be automatically synchronised with data in *Sleuth*.

  Sleuth use a product provided by Groupcall called *Xporter* to synchronise data; this involves the export of data from the school's MIS which is then imported into *Sleuth*. The school, as the data controller manage the login credentials to access MIS data. SSC, as the data processor provide the school with the login credentials to import the data into *Sleuth*.

- **ISSUE:** Understanding the cloud-based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: SSL is the standard security technology for creating a secure encrypted link between a web server and a browser. Data passed between the browser and *Sleuth* is private and secure. SSL is an industry standard used by millions of websites in the protection of their online transactions with their customers.

- **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: *Sleuth* servers are 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: All users have a unique username and password that they can reset at any time. All users select their own memorable keyword from which 2 letters are requested at random each time they log on unless this has been disabled by the request of the school.

  A user has a limited number of opportunities to login before they are forced to wait for a period of time before trying again. This prevents any automated processes attempting multiple combinations to login.

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: SSC processes data on behalf of the school for the duration of the agreed contract, typically one or three years. Towards the end of this period the school will be offered a contract renewal and reminded of SSC compliance with GDPR practices. If the school do not intend to renew then the school can extract and save any data it wishes to retain before the contract ends. SSC will not process school data beyond this time.

  When the school contract expires the data will be retained for one month before deletion. SSC will retain an encrypted version of the data for up to six months as part of its backup systems. After this period, all the data will be deleted from *Sleuth* servers and no electronic or physical copies of the data will be held by SSC or shared with any other party.

  The school will be advised about options for retaining its own copy of data from *Sleuth* before the end of the contract. SSC takes no responsibility for the security of data the school choose to print or export from *Sleuth* and retain elsewhere, either during the contract or after the end of the school's contract period with *Sleuth*.

- **ISSUE:** Data Back ups
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: There are full nightly backups of your entire school's *Sleuth* data. Backups are held securely inside our datacentre and also transferred over a secure connection to an offsite location where they are stored securely in an encrypted form.

In addition to the nightly backups, we run a transactional log on all our *Sleuth* databases that records every transaction to a local file so in the event of a database failure we can restore all data up to the second the database stopped working. This should result in no data being lost.

Hardware redundancy – SSC have multiple web and database servers so should any one server go down there is always another to continue running *Sleuth*. SSC run *Sleuth* across 2 geographically separate data centres in the UK, so should a whole data centre suffer any kind of issue the *Sleuth* traffic is routed to the working data centre automatically with no loss of service.

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: In the event of a breach which affects school data, SSC will inform the school as soon as possible after it has been discovered. This will allow the school to assess its position and liaise with the Information Commissioner's Office or other relevant entities.

- **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: Under the GDPR, all individuals who are the subject of personal data held by *Sleuth* are entitled to obtain (1) confirmation that *Sleuth* are processing their personal data; (2) a copy of their personal data; and (3) other supplementary information.

  Sleuth will provide school administrators with an automated subject access requests routine that will enable them to retrieve data related to students, teachers and parents in the system.

  If *Sleuth* receive any requests directly, *Sleuth* may pass these back to the school's *Sleuth* administrator where relevant or will provide the requested information within 30 days of the request (provided *Sleuth* can verify the identity and authority of the person making the request).

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance

MITIGATING ACTION: The school as data controller retains ownership of the data. *Sleuth* is the data processor.

- **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: SSC have multiple web and database servers so should any one server go down there is always another to continue running *Sleuth*. SSC run *Sleuth* across 2 geographically separate data centres in the UK, so should a whole data centre suffer any kind of issue the *Sleuth* traffic is routed to the working data centre automatically with no loss of service.

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

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: A secure login is required to access the data in *Sleuth*. Data is securely stored on a web server in the United Kingdom (UK). Secure connections are used to encrypt and decrypt data moving between the web server and *Sleuth*. Regular backups of school data are held securely. Hardware redundancy measures are taken to protect from data loss.

  All users have a unique username and password that they can reset at any time. All users select their own memorable keyword from which 2 letters are requested at random each time they log on unless this has been disabled by the request of the school.

  A user has a limited number of opportunities to login before they are forced to wait for a period of time before trying again. This prevents any automated processes attempting multiple combinations to login.

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 a cloud-based solution will realise the following benefits:

- Scaleability
- 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 (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
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 UK, HTTPS and SSL encryption	Reduced	Medium	Yes
Data Breaches	Where applicable 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:	Miss Tina Partridge	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Miss Tina Partridge	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: Schools should be aware of the privacy issues and ensure these are upheld if they intend to use *Sleuth*.		
DPO advice accepted or overruled by: Yes If overruled, you must explain your reasons		
Comments:		
Consultation responses reviewed by: Senior Leadership Team If your decision departs from individuals' views, you must explain your reasons		
Comments:		
This DPIA will kept under review by:	Miss Tina Partridge	The DPO should also review ongoing compliance with DPIA