Data Protection Impact Assessment (Satchel One)

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. Summerhill School operates a cloud based system. As such Summerhill School must consider the privacy implications of such a system.

The Data Protection Impact Assessment is a systematic process for identifying and addressing privacy issues and considers the future consequences for privacy of a current or proposed action.

Summerhill School recognises that moving to a cloud service provider has a number of implications. Summerhill School recognises the need to have a good overview of its data information flow.

The Data Protection Impact Assessment looks at the wider context of privacy taking into account Data Protection Law and the Human Rights Act. It considers the need for 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 GDPR is satisfied by the school.

Summerhill School aims to undertake this Data Protection Impact Assessment on an annual basis.

A Data Protection Impact Assessment will typically consist of the following key steps:

1. Identify the need for a DPIA
2. Describe the information flow
3. Identify data protection and related risks
4. Identify data protection solutions to reduce or eliminate the risks
5. Sign off the outcomes of the DPIA

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

What is the aim of the project? –Satchel One is a digital student planner that lets the school easily track classes, homework, tests and projects. Its primary purpose is to provide a platform for the accessing and sharing of school work between teachers and students. As such it delivers a cost effective solution to meet the needs of the business.

Teachers

- Class Details – Teachers can quickly share their class information on Teachers.io
- Syllabus – Teachers can upload or enter their syllabus in Teachers.io
- Assignments – Teachers enter assignments, tests and lessons on Teachers.io and each student's planner is automatically updated
- Attachments & Resources – Teachers can share files and links with their students. This makes it very easy for students to find the files and information they need for each assignment
- Announcements – Teachers can make announcements to their classes and Satchel One will notify each student
- Contact Information – Teachers can share their contact information to make it easy for parents and students to reach them at the right place and time
- Teacher Profile – Teachers can share information what schools they attended, articles and books they've published, awards they've received and more

Students

- Students can easily join their class in Satchel One to automatically get information the teacher shares synced to the student planner
- Students can easily access the syllabus even if they don't have an internet connection.
- Student planner updated
- Students will have access to files and resources to undertake their homework
- Satchel One will notify each student regarding any school announcements

Satchel One app is accessible via the iPhone, iPad, Android, Windows 8, Kindle Fire and the Web.

Summerhill School will undertake the following processes:

1. Collecting personal data
2. Recording and organizing personal data
3. Structuring and storing personal data
4. Copying personal data
5. Retrieving personal data
6. Deleting personal data

By opting for 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 and workforce) for the school provides the lawful basis of why the school collects data. **How will you collect, use, store and delete data?** – The information collected by the school is retained on 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?** – Summerhill 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. Summerhill School routinely shares workforce information internally with people responsible for HR and recruitment (including payroll), senior staff, with the Local Authority, and the Department for Education. **What types of processing identified as likely high risk are involved?** – Transferring 'special category' data from the school to the cloud. Storage of personal and 'special category data in the Cloud. However, in terms of using Satchel One no special category data will 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 (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 (doctors 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 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, RM Integris, child safeguarding files, SEN reports, etc. However, in terms of using Satchel One no special category data will be used. **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? – Satchel One 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 schools management information system.

Teachers.io is the faculty companion app to Satchel One. It allows teachers to share information about themselves and their classes so Satchel One users can join their class and automatically download the information the teacher shares.

When a student joins a class, the only information the teacher sees is to help identify & understand the basic usage of the Satchel One users that have joined their class and includes username, email, and names if available.

Additional information regarding student usage of Show Satchel One may be shared with teachers at the school. The student gives the school access to their information by either signing up with the school owned account or explicitly granting permission in Satchel One.

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

Through the Privacy Notice (student/workforce) Summerhill School is committed to being transparent about how it collects and uses data and to meeting its data protection obligation. Satchel is able to support the school's obligations under 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.

The teacher can set up individual user accounts enabling pupils to receive assignments and have them marked. Each account will have the class/year of the pupil and their first and last name.

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? – None of the data in Satchel One will have special category data such as child safeguarding records, SEN records, Single Central Record.

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 inasmuch as the encryption key will need to be shared with others to access the data.

Summerhill School recognises that moving to a cloud based solution raises a number of General Data Protection Regulations issues as follows:

- **ISSUE:** The cloud based solution will be storing personal data including sensitive information
  RISK: There is a risk of uncontrolled distribution of information to third parties
  MITIGATING ACTION: Satchel One and the school's personal data are stored on approved and compliant cloud infrastructure. Satchel One servers are hosted by Amazon Web Services (AWS) in Ireland to ensure customer data is retained within the European Economic Area (EEA). AWS use multiple protective layers within its platform to protect Satchel One services, including encryption and firewalling. Satchel One have completed a full 3rd-party audit.

  Satchel One store business data within selected cloud platforms, including services like Google Drive and Salesforce. Satchel One will only use platforms whose information security practices Satchel One approve
  ISSUE: Transfer of data between the school and the cloud

RISK: Risk of compromise and unlawful access when personal data is transferred
MITIGATING ACTION: Satchel One uses HTTPS (Hypertext Transfer Protocol Secure) for all transmissions between the school and Satchel One servers

All data transfers use SHA256 with RSA (RSA 2048 bits for key exchange) between client browsers and Satchel One servers.

All data is encrypted

- **ISSUE**: Security of data whilst hosted in the cloud
  RISK: Risk of compromise and unlawful access when personal data is at rest
  MITIGATING ACTION: Where it is necessary to access personal data, for example to investigate a support case, only approved Satchel *(owners of Satchel One)* support and technical staff can access it

  Satchel carries out DBS checking on staff who have personal data access and staff are subject to contractual data access policies

- **ISSUE:** Use of third party sub processors?
  RISK: Non compliance with the requirements under GDPR
  MITIGATING ACTION: Satchel is an ICO registered company under Teachercentric Limited (registration number ZA009602). It is compliant with GDPR with the application of appropriate model contract clauses to ensure compliance by third party sub processors

- **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: All data flowing across the AWS global network that connects AWS datacenters and regions is automatically encrypted at the physical layer before it leaves AWS's secured facilities. Additional encryption layers exist as well; for example, all VPC (Virtual Private Cloud) cross-region traffic, and customer or service-to-service TLS connections

- **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: Satchel One servers are hosted by Amazon Web Services (AWS) in Ireland to ensure customer data is retained within the European Economic Area (EEA)

If Satchel transfer personal data from the EU to an organisation in the United States it will determine that the organisation is signed up with the Privacy Shield framework. It will also ensure that the appropriate data processing agreements are in place with standard GDPR clauses

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. The school will need to confirm whether an SCC is in place.

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: GDPR non-compliance
  MITIGATING ACTION: Satchel is able to support the school in its obligations with regards to a user exercising their data subject's rights, for example if they were to make a Subject Access Request (SAR) to the school acting as the data controller

  If a data subject wishes to make a Subject Access Request and/or Right to be Forgotten request, where applicable, the school can contact gdpr@teamsatchel.com on behalf of the requestor

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: GDPR non-compliance
  MITIGATING ACTION: Satchel will process and store personal data for students, parents, teachers and school staff members for the duration of the schools license with Satchel. If a student/teacher leaves the school during an active license with the school Satchel will delete/anonymise personal data within 28 days of the account being deleted by the school

ISSUE: Responding to a data breach
RISK: GDPR non-compliance

MITIGATING ACTION: Satchel is an ICO registered company under Teachercentric Limited (registration number ZA009602). It is compliant with GDPR data security handling and reporting

- **ISSUE:** No deal Brexit
  RISK: GDPR non-compliance
  MITIGATING ACTION: If a Withdrawal Agreement is concluded, in principle the GDPR would continue to apply in the UK until the end of 2020 (the currently stipulated 'transition period'). In this case, nothing would change for the way in which Satchel One processes personal data, which is currently carried out in accordance with the GDPR under UK law

  In the event of a no deal Brexit the UK will be outside of the European Economic Area ("EEA") at the time of exit. With regards to Satchel One's use of the AWS in Ireland, the UK will transitionally recognise all EEA states, EU and EEA institutions, and Gibraltar as providing an adequate level of protection for personal data. This means that personal data can continue to flow freely from the UK to these destinations following the UK's exit from the EU

  As a further contingency in the event of any currently unforeseen scenario, Satchel One could be hosted through the London AWS instance in the event that it is required that we host certain data within the UK

- **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: Satchel is able to support the school in its obligations with regards to a user exercising their data subject's rights, for example if they were to make a Subject Access Request (SAR) to the school acting as the data controller

  If a data subject wishes to make a Subject Access Request and/or Right to be Forgotten request, where applicable, the school can contact gdpr@teamsatchel.com on behalf of the requestor

- **ISSUE:** Data Ownership
  RISK: GDPR non-compliance
  MITIGATING ACTION: The school as data controller retains ownership of the data. Satchel One 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: AWS use multiple protective layers within its platform to protect Satchel One services, including encryption and firewalling. Satchel One have completed a full 3rd-party audit

- **ISSUE:** Security of Privacy
  RISK: GDPR non-compliance
  MITIGATING ACTION: The owners of Satchel One are registered with the ICO under Teachercentric Limited (registration number ZA009602)

  AWS Data Centers are ISO27001 accredited.

  ISO 27001: is one of the most widely recognized, internationally accepted independent security standards. AWS has earned ISO 27001 certification for the systems, applications, people, technology, processes, and data centres that make up its shared Common Infrastructure

  AWS computing environments are continuously audited, with certifications from accreditation bodies across the world, including FedRAMP, DoD CSM, and PCI DSS

  AWS is also fully compliant with applicable EU Data Protection laws, and the AWS Data Processing Agreement incorporates the Article 29 Working Party Model Clauses

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 (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 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
No deal Brexit	Possible	Significant	Medium
Subject Access Request	Probable	Significant	Medium
Data Retention	Probable	Significant	Medium

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no
Data Transfer	Secure network, end to end encryption	Reduced	Medium	Yes
Asset protection & resilience	Data Centre in EU, Certified, Penetration Testing and Audit	Reduced	Medium	Yes
Data Breaches	Where applicable documented in contract and owned by school	Reduced	Low	Yes
No deal Brexit	Contingency plans in place	Reduced	Low	Yes
Subject Access Request	Technical capability to satisfy data subject access request	Reduced	Low	Yes
Data Retention	Implementing school data retention periods in the cloud	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Martyn Palfreyman	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Martyn Palfreyman	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Yes	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Concerns have been raised about third party access (see TES Exclusive: School app scraps ads over privacy concerns) to the Satchel One platform. Schools should be aware of the privacy issues and ensure these are upheld if they intend to use Satchel One		
DPO advice accepted or overruled by:	**[Yes/No]**	If overruled, you must explain your reasons
Comments: **[DPO Advice provided]**		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments: **[Comments provided]**		
This DPIA will kept under review by:	Vicki Poole	The DPO should also review ongoing compliance with DPIA