Data Protection Impact Assessment (School SCR)

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 UK 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.

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.

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 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

The single central record is a key requirement for all schools and colleges. It plays a vital role in ensuring the safety and wellbeing of your students. The school must record all DBS checks, qualifications, and other essential staff information in your single central record.

The single central record is a record of all the recruitment, identity, and vetting checks conducted on school staff. This includes teachers, support staff, volunteers, Governors, and anyone else who has access to children. Traditionally, schools have used spreadsheets to maintain their single central record.

Increasingly, schools are turning toward software solutions to more effectively manage their Single Central Record. The Single Central Record acts as a record for a range of essential vetting and personnel checks. It must include:

1. Identity Checks

Purpose: To ensure that the person is who they say they are.
Importance: Verifying true identities ensures that individuals cannot bypass the vetting system using false identification.

A valid passport or driver's license is required for an identify check. This should be presented in-person by an applicant. The school should take a photo or digital copy of this. It is also best practice to verify the applicant's address.

2. Qualification Checks

Purpose: To validate that the person holds the required qualifications for the job. This includes **Qualified Teacher Status (QTS)** and a **Teacher Reference Number** (TRN).
Importance: In state funded schools, it is a legal requirement for teachers to hold a relevant qualification.

3. Enhanced DBS Checks

Purpose: To uncover any cautions, warnings, reprimands, and relevant information from police records, beyond just convictions.
Importance: **The Police Act 1997** mandates Enhanced DBS checks for roles involving unsupervised and regular contact with children.

4. Barred List Checks

Purpose: To verify that the person isn't on the Children's Barred List, preventing them from working with children.
Importance: This check originates from the **Safeguarding Vulnerable Groups Act 2006**. The Children's Barred List was previously known as List 99.

5. Prohibition Checks

Purpose: This is to verify that the person hasn't been banned from teaching.
Importance: The **National College for Teaching and Leadership** (NCTL) maintains a database of individuals barred from teaching.

6. Section 128 Checks

The Section 128 Check applies to school leadership positions, governors, and trustees.

Purpose: To verify that the person hasn't been barred from school management roles.
Importance: Section 128 (**Education and Skills Act 2008**) grants the Secretary of State the power to ban an individual from school management. There are a variety of reasons this may occur and this ban will not show up on an Enhanced DBS check. That is why it's vital to always complete a Section 128 check for management and governance applicants.

7. Right to Work Checks

Purpose: To verify that the person has the legal right to work in the UK through documentation such as their passport or visa.
Importance: It is a universally required check for all UK employers (**Immigration, Asylum, and Nationality Act 2006**).

8. Overseas Checks

This is only required when a person has worked abroad.

Purpose: To verify that the person has no foreign convictions or teaching prohibitions.
Importance: The applicant should provide the school with a Certificate of Good Character. This is an official document from their country of residence to prove they have no convictions. The format varies by country. The **UK Government website** has further guidance on this.

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 workforce data in the cloud.

The Single Central Record Tracker Software improves how schools manage their SCR. The benefits include the following:

Streamlines compliance management – By ensuring that all mandatory data and checks are accurately maintained and easily accessible, single central record tracker software significantly improves compliance. By automating updates and alerts, software reduces the administrative burden on staff and minimises the risk of human error.

Saves time through automations – Single central record software allows the school to order vetting checks through the platform. This helps automate the entry, collection, and verification of staff data. In addition, SCR software can automatically undertake compliance audits, highlighting any issues the moment they occur. This minimises many of the manual tasks involved in managing the SCR.

Improves Reporting – SCR software has the ability to generate reports, making it easier to demonstrate compliance at a moment's notice. This is particularly useful for reporting to governors and Ofsted.

Improves data security – SCR uses advanced encryption and secure access protocols to ensure data security. School SCR use 256-bit 'bank grade' encryption to do this. This ensures the school regularly back up its data to prevent loss in case of hardware failures or cyber-attacks.

Inbuilt vetting checks – Having the ability to order DBS and personnel vetting checks from within School SCR tracker saves time. This feature automates the verification of background checks, qualifications, and other critical data against official databases and records.

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 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 (Workforce) 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 Summerhill School Privacy Notice (Workforce) 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? – 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 workforce information internally with people responsible for HR and recruitment (including payroll), senior staff, with the Local Authority, Department for Education, and Ofsted.

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? – 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. Information about medical or health conditions.

Special Category data? – Some of the personal data collected falls under the UK GDPR special category data. This includes race; ethic origin; religion; and health. These may be contained in the Single Central Record.

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 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 (workforce, governors, and volunteers)? 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. Information about medical or health conditions.

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 employees to manage the employment relationship.

Through the Privacy Notice (Workforce) Summerhill 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. School SCR is hosting the data and has the ability to access data on instruction of Summerhill 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 School SCR will update the data stored by the school.

Do they include children or other vulnerable groups? – Some of the data may include special category data such as gender, age, ethnic group.

Are there prior concerns over this type of processing or security flaws? – School SCR uses Amazon Web Services (AWS) in the UK. AWS are ISO 27001 accredited, the international standard for information security management.

Summerhill 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 data is stored within AWS London data centres. Security is as follows: Restricted, authorised access only. Biometric access with multi-factor authentication, 24/7 surveillance with intrusion detection systems. Perimeter security

with guard stations on entrances. Redundant power and cooling systems. Virtual firewalls and intrusion detection/prevention systems monitor and block unauthorised network traffic.

Multi-Tenant Isolation: AWS employs logical isolation mechanisms to prevent customer data from being accessed by other customers. AWS employs logical isolation mechanisms to prevent customer data from being accessed by other customers

- **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 data is encrypted at rest and in transit using TLS 3 AES 128 bit encryption. All School SCR servers are situated in secure locations.

  Sensitive data is protected and encrypted to the highest levels giving ensuring GDPR compliance

- **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 School SCR 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: No other 3rd party has access to a customer's Personal Identifiable Information held within the single central record

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: School SCR is fully compliant with UK GDPR data security retention and storage. School SCR 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. School SCR 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:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: School SCR Ltd is a full member of the ICO and complies with the ICO's data breach procedure. All employees are trained and aware of this procedure.

- **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: School SCR has the functionality to respond to Subject Access Requests. School SCR 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. School SCR is the data processor

- **ISSUE:** Data is not backed up
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: School SCR Ltd backs up customer data every 24 hours and keeps 10 days of backups available. Backup rotation takes place every 10 days, with the new backup replacing the first backup. Data can be deleted quicker upon written

request if required. Our data centre availability is 99.9% and data is encrypted, partitioned, and stored across multiple servers reducing any single point of failure

In the unlikely event of a data outage, data can be restored within 24 hours once the data centre is back online. AWS conducts regular and robust security updates, with server security amongst the best in the world

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: School SCR is hosted on UK servers

- **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, School SCR is UK GDPR compliant. The data processor remains accountable for the data within the system. For the services it manages, School SCR applies its own security updates. Where security updates are applicable to the infrastructure, Amazon Web Services will manage these

  AWS conducts regular recovery simulations and maintains rapid recovery capabilities. AWS carries out regular penetration testing on its data centre to identify and patch any weaknesses

- **ISSUE:** Third-party Access to Data
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: No subcontracting takes place at School SCR Ltd

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

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance

MITIGATING ACTION: School SCR Ltd has various security procedures in place which ensure the safety of the school's data as noted above. Others include:

ICO Registration: School SCR Ltd 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. The registration number is ZB665448

All data is stored and hosted on AWS who hold the following certifications:

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

ISO 27017: is an international standard of practice for information security controls based on ISO/IEC 27002, specifically for Cloud Services. AWS has been certified compliant with ISO 27017 for its shared Common Infrastructure

ISO 27018: is an international standard of practice for protection of personally identifiable information (PII) in Public Cloud Services. AWS has been certified compliant with ISO 27018 for its shared Common Infrastructure

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 (Workforce). The lawful 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
Processing by Artificial Intelligence	Technical and organisational measures	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Vicki Poole	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Vicki Poole	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:

1. Do any staff employed by SCR Ltd receive training in regard to data protection, linked to their duty of confidentiality or have DBS clearance? Is access to customer data granted on a role / permissions-basis?
2. Are all SCR Ltd employees aware of the company data breach procedure?
3. Does SCR Ltd subcontract or not? And if so, do they meet the same standards of data protection / GDPR as yourselves?
4. Is data encrypted between the school and the SCR Ltd server. If you use SSL encryption, could you advise what standard it meets (e.g. TLS 1.2 / AES-256bit)?
5. Where is the server located which hosts data from the school? (i.e. the UK)?
6. What service ISO certifications for the hosting of data (i.e. do you as a company hold ISO 27001 or is it the hosting company that holds the certification)?
7. What physical access controls exist, security of the servers, permission-based access, CCTV recording, Cyber Essentials certification, vulnerability and penetration testing.
8. Should demand unexpectedly increase, can your server hosting service scale their facilities to meet demand?
9. What resiliency does the server hosting service provide for the availability of data? E.g. mirrored data centres, how often are backups taken and how long would it take to restore from an outage? Does the service manage all security updates for the service?
10. Is the SCR Ltd data encrypted at rest on the hosting servers?

<table>
<tr><td colspan="3">11. Where the school may have deleted data and SCR Ltd holds the data on a backup, how long would it take for that data to be deleted from the backup? i.e. what is the backup rotation period if backups are overwritten?
Responses to the above questions have been embedded in the Issue, Risk and Mitigation log of this DPIA.</td></tr>
<tr><td colspan="3">DPO advice accepted or overruled by:
Vicki Poole If overruled, you must explain your reasons</td></tr>
<tr><td colspan="3">Comments:</td></tr>
<tr><td colspan="3">Consultation responses reviewed by:
If your decision departs from individuals' views, you must explain your reasons</td></tr>
<tr><td colspan="3">Comments</td></tr>
<tr><td>This DPIA will kept under review by:</td><td>Vicki Poole</td><td>The DPO should also review ongoing compliance with DPIA</td></tr>
</table>