Data Protection Impact Assessment (Arbor)

Sheriffhales Primary School & Preschool operates a cloud-based system. As such Sheriffhales Primary School & Preschool 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.

Sheriffhales Primary School & Preschool recognises that moving to a cloud service provider has a number of implications. Sheriffhales Primary School & Preschool 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 cloudbased 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.

Sheriffhales Primary School & Preschool 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 14

Step 5: Identify and assess risks 16

Step 6: Identify measures to reduce risk 17

Step 7: Sign off and record outcomes 18

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. Sheriffhales Primary School & Preschool will undertake the following processes:

1. Collecting personal data
2. Recording and organising 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

Arbor is a cloud-based system, which enables the school to manage student information in a variety of ways through three broad modules. Module (1) MIS Core, which include attendance, behaviour, progress tracking and school census. Module (2) MIS Comms, which include Parental Portal, Parents Evening Booking, Arbor App.

Module (3) MIS Perform, which include Curriculum Tracking, Payments, Meal Management and Intervention Tracking. Functionality includes the following:

- **Communications**: Send and receive e-mail and SMS messages
- **Report Builder:** building reports using data from Arbor
- **Payments**: Management of online and offline payments for meals, clubs and trips. Easily schedule activities and link them to payments and consent
- **Safeguarding**: securely permissioned access to special category safeguarding data including SEN. Record and report on attendance. Add interventions and monitor for effectiveness
- **Staff and HR**: keeping track of staff absences, appraisals and objectives

In addition, Arbor has the ability to integrate with a number of third-party systems including Wonde, and CPOMS.

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 student 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 (student 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? – Student information is collected via registration forms when students join the school, student update forms the school issue at the start of the year, Common Transfer File (CTF) or secure file transfer from previous schools. Student 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? – Sheriffhales Primary School & Preschool routinely shares student information with relevant staff within the school, schools that the student attends after leaving, the Local Authority, the Department for Education, Health Services, Learning Support Services, Arbor and various third party Information Society Services applications. Sheriffhales Primary School & Preschool 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 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? – Student data relates to personal identifiers and contacts (such as name, unique student 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 falls under the UK GDPR special category data. This includes race; ethic origin; religion; biometrics; and health. These may be contained in the Single Central Record, Arbor, child safeguarding files, SEN reports, etc.

How much data is collected and used and how often? – Personal data is collected for all students. Additionally, personal data is also held respecting the school's workforce, Board of Governors, Volunteers, and Contractors. Data relating to sports coaches and other

Do they include children or other vulnerable groups? – Some of the data may include special category data such as child safeguarding records, Arbor, SEN records, Single Central Record. The cloud service provider may provide access controls to the files. For example, files designated as private – only you can access the files; public – everyone can view the files without any restriction; and shared – only people you invite can view the files.

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

Sheriffhales Primary School & Preschool 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 Arbor have their own accounts. Arbor servers are patched continuously to reduce security vulnerabilities

- **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 256 bit SSL encryption. All Arbor 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: All data is encrypted at rest and in transit using 256 bit SSL encryption. All Arbor servers are situated in secure locations. Physical security is maintained at every Arbor office using access control, secure keys, and secure perimeter doors

- **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 Arbor 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 Arbor, and they employ a 'least privilege' code of practice within our organisation Arbor have various security procedures in place which ensure the safety of school data within Arbor's ISO 27001 system, and the database is only accessed with express permission from the school Arbor offer a range of additional security features, including password rules, enforced regular password changes, and two-factor authentication. Arbor also automatically logs out after a period of inactivity Arbor lock down access to its databases to specific individuals and only allow access through strict gateways requiring two-factor authentication login and public/private key identification. All logins to Arbor are logged and tracked, and strict policies are enforced which create alerts if breached. Staff passwords are also changed regularly and, since data is kept on Arbor's central system, permissions can easily be revoked if needed DPIA (Arbor) v1.1 20221014 10

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Arbor is fully compliant with UK GDPR data security retention and storage. Arbor 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. Arbor 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: Arbor is an ICO registered company, fully compliant with UK GDPR data security handling and reporting

- **ISSUE:** Data Retention
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Arbor has a policy where data is retained for as long as necessary to provide the service Arbor will automatically flag records that have passed the school's data retention period, meaning the school can easily find and remove all students (and staff) who left the school more than six years ago

- **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: Arbor has the functionality within the reports module to respond to Subject Access Requests. Arbor agrees to comply with Subject Access Requests relating to the data it stores A complete record of all personal data stored on Arbor via a student or staff member profile page can be downloaded DPIA (Arbor) v1.1 20221014 11

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

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Arbor 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, Arbor is UK GDPR compliant. The data processor remains accountable for the data within the system. For the services it manages, Arbor 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 Arbor, to third-party applications, the school must give explicit authorisation 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 Arbor in strict compliance with ISO 27001 and agree to abide by the Arbor data sharing and confidentiality policies DPIA (Arbor) v1.1 20221014 12

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

Cyber Essentials: Cyber Essentials is a government-backed certification scheme designed to protect organisations from 80% of common cyber-attacks and increase cyber security Arbor are certified with Cyber Essentials and are audited annually. This means Arbor IT systems are security approved by an accreditation body selected by the NCSC and Arbor have technical defences in place against cyber threats

ICO Registration: Arbor 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 Z3022381

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

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 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 risks

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 Subject	Documented in contract and owned by school	Reduced	Low	Yes
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:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Yes	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by: If overruled, you must explain your reasons		
Comments:		
Consultation responses reviewed by: If your decision departs from individuals' views, you must explain your reasons		
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA