Data Protection Impact Assessment (School Admissions Management)

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. Blanford Mere Nursery & Primary School operates a cloud based system. As such Blanford Mere Nursery & Primary School must consider the privacy implications of such a system. The Data Protection Impact Assessment is a systematic process for identifying and addressing privacy issues and considers the future consequences for privacy of a current or proposed action.

Blanford Mere Nursery & Primary School recognises that moving to a cloud service provider has a number of implications. Blanford Mere Nursery & Primary School recognises the need to have a good overview of its data information flow. The Data Protection Impact Assessment looks at the wider context of privacy taking into account Data Protection Law and the Human Rights Act. It considers the need for a cloud based system and the impact it may have on individual privacy.

The school needs to know where the data is stored, how it can be transferred and what access possibilities the school has to its data. The location of the cloud is important to determine applicable law. The school will need to satisfy its responsibilities in determining whether the security measures the cloud provider has taken are sufficient, and that the rights of the data subject under the UK GDPR is satisfied by the school.

Blanford Mere Nursery & Primary School aims to undertake this Data Protection Impact Assessment on an annual basis. A Data Protection Impact Assessment will typically consist of the following key steps:

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

Contents

Step 1: Identify the need for a DPIA

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

What is the aim of the project? – Managing school admissions is complex and time-consuming for local authorities, schools and parents.

The school uses Synergy's School Admissions Management admissions solution (owned by the Access Group) produced by the company Servelec which enables parents to apply for school places online, thereby removing the need for local authorities and schools to spend a large amount of time entering data.

Synergy manages the admissions, transfers and appeals processes across all schools and key stages from nursery to secondary school, along with transfers and in-year admissions.

The school management software records details of school capacities, applications for places, decisions and automatic allocations based on specified criteria against admissions policies. Synergy provides a powerful and flexible search and selection process, so school place applications can be quickly retrieved and updated.

Modules within Synergy's School Admissions Management solution include the following:

Admissions Management: Admissions Management is a Windows based application that records details of school capacities, attendance applications, appeals and placements. It provides a comprehensive online schools admission system.

Synergy allows for powerful and flexible search and selection of school place applications, efficient bulk processing based on the admissions criteria for either the local authority or the individual school, and it can run stand alone or as a part of the integrated suite of software.

Synergy Parent Portal: Parents can apply for school places online using the Synergy Parent Portal, which can also be accessed on mobile devices. Parents can view all the information they need and make their preferences quickly with validations in place to help them enter the correct information. Parents are kept up-to-date with their application in the portal, and are able to accept/decline offers and appeal decisions.

School Access: Using Synergy's school access control system, schools can view all applications to them, including all parent-supplied information via the Parent Portal. Schools are able to securely download all pupil information for import into their Management Information System (MIS) at the end of the enrolment process.

Own Admissions Authority Schools can rank applicants online with the local authority able to see this in real-time.

Primary Schools are able to see whether their pupils have made preferences and can support parents where necessary.

Geographical Information System Software: The Geographical Information System (GIS) software extension will retrieve catchment area data for the applicant and can generate catchment-based preferences. Using GIS for school management gives Blanford Mere Nursery & Primary School an online distance measurement, in straight line route, shortest calculated route and safe walking routes, including details of catchment areas and nearest school type details.

Electronic Data Exchange: The Electronic Data Exchange Module (EDEM) utilises user-friendly wizard-based tools to handle the import and export of all Department for Education prescribed files. Online modules are available for pupils to apply for school places and for schools to manage applications. These are real e-government applications that will benefit both the applicants and the local authority; to support co-ordinated admissions and transfers.

The use of School Admissions Management (SAM) will help the school to deliver a cost effective solution to meet the needs of the business.

Blanford Mere Nursery & Primary School will undertake the following processes:

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

By opting for 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 school can easily upload personal data to the cloud. The information can be accessed from any location and from 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.

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 also stored in the cloud. 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.

Will you be sharing data with anyone? – Blanford Mere Nursery & Primary 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.

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 School Admissions Management the use of special category data will limited to the lawful basis as outlined in the school's Privacy Notice (Pupil).

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, home address). Characteristics (gender (siblings, siblings gender, siblings date of birth), Court Order, Education Health Care Plan (EHCP), Looked After Child (LAC)). School Preference and reasons for school choice and distance from home to school. The school also obtains data on parents/guardians/carers including their name, address, telephone number and e-mail address.

Special Category data? – Some of the personal data collected falls under the UK GDPR special category data. This includes health. In terms of using School Admissions Management.

The lawful basis for collecting this information relates to Article 9 2 (b) *processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorized by domestic law (see section 10 of the 2018 Act) or a collective agreement pursuant to domestic law providing for appropriate safeguards for the fundamental rights and interests of the data subject.*

Whatever special category data is used the school will ensure that it has a lawful basis to do this and that this is documented in the school's Privacy Notice (Pupil).

How much data is collected and used and how often? – Personal data is collected for all pupils.

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? – How many individuals are affected (pupils, workforce, governors, volunteers)? And what is the geographical area covered? Reception, Year 1 to Year 6 pupils. School Admissions Management will be used by the school to help parents to apply for school places online. It will also manage the admissions, transfers and appeals processes across all schools and key stages from nursery to secondary school, along with transfers and in-year admissions.

The school will act as in accordance with the lawful basis it has for using personal data. This is outlined in the schools Privacy Notice (Pupil).

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? – Blanford Mere Nursery & Primary School collects and processes personal data relating to its pupils to manage the school and parent/pupil relationship.

Through the Privacy Notice (Pupil) Blanford Mere Nursery & Primary School is committed to being transparent about how it collects and uses data and to meeting its data protection obligation.

How much control will they have? – Access to the files will be controlled by username and password. 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? – In terms of using School Admissions Management special category data may be collected to assist in the enrolment process.

Whatever special category data is used the school will ensure that it has a lawful basis to do this and that this is documented in the school's Privacy Notice (Pupil).

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.

Blanford Mere Nursery & Primary 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: Server is hosted in Node 4 with restricted access to the

servers/data. Node 4 includes perimeter fencing, CCTV, photo ID, 24/7 manned security, anti-pass-through data centre entry, and caged areas available

Access Group complete annual penetration testing, and is Cyber essentials accredited.

Access Group are currently ISO27001 certified, and they undertake to maintain this certification for the Licence Term. ISO27001 certification demands best in class controls across: Information security policies, organisation of information security, human resource security, asset management, access control, cryptography, physical and environmental security, operations security, communications security, system acquisition, development and maintenance, supplier relationships, information security incident management, information security aspects of business continuity management, and compliance; with internal requirements, such as policies, and with external requirements, such as laws

ISSUE: Transfer of data between the school and the cloud
RISK: Risk of compromise and unlawful access when personal data is transferred.
MITIGATING ACTION: Encryption is identified in the UK GDPR as a protective measure that renders personal data unintelligible when it is affected by a breach

The browser utilises TLS 1.2 encrypted connections through a portal

Data is encrypted at rest, RBAC in place which can be managed by allocating individuals at customer levels. Internally access to data is restricted to those that are required to support the system, only accessed internally via VPN and secure RDS connection

ISO27001 certification demands best in class controls across: Information security policies, organisation of information security, human resource security, asset management, access control, cryptography, physical and environmental security, operations security, communications security, to comply such as laws

- **ISSUE:** Use of third party sub processors?
  RISK: Non compliance with the requirements under UK GDPR
  MITIGATING ACTION: School Admissions Management may have to ad hoc share the schools personal data with regulators, law enforcement bodies, government agencies, courts or other third parties where Access Group think it's necessary to comply with applicable laws or regulations, or to exercise, establish or defend Access Group legal rights

  Access Group have also partnered with reputable third parties to provide a best-in-class service offering to the school and its wider customer base

Access Group may also share school personal data with other members of the Access Group: the Access Group will only do this where they have a lawful basis for doing so, for example, contract or legitimate interests. Where the receiver of the schools personal data is an Access Group entity which is outside of the UK (or the EU, in the case of EU personal data), the transfer will be safeguarded by, at minimum, an intra-group agreement (which includes recognised model clauses)

Where sharing schools personal data with Access Group trusted partners means transferring your personal data outside of the UK or European Union Access Group will ensure they put in place appropriate safeguards and supplementary measures (where necessary)

- **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: ISO27001 certification demands best in class controls across: Information security policies, organisation of information security, human resource security, asset management, access control, cryptography, physical and environmental security, operations security, communications security, system acquisition, development and maintenance, supplier relationships, information security incident management, information security aspects of business continuity management, and compliance; with internal requirements, such as policies, and with external requirements, such as laws

- **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: Servers are UK based

  However, the UK has been granted an adequacy decision from the EU, meaning the laws and practices of the UK have been found to offer an essentially equivalent level of protection to personal data as is granted in the EU.

  In the event the adequacy decision is revoked or expires (without renewal) and to ensure continuity of service for Access Group customers, they have incorporated the Standard Contractual Clauses (SCCs) into customer contracts, accessible via Access Group Brexit update (available here).

  The SCCs shall sit silent until and unless they are required to be put in place by either the UK or EU GDPR

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: When operating as a processor, Access Group makes available to schools, as data controllers, the personal data of its data subjects and the ability to fulfill data subject access requests when they exercise their rights under the UK GDPR This is done in a manner consistent with the functionality of the product and Access Group's role as a data processor

  If Access Group receive a request from the school's data subjects to exercise one or more of their rights under the UK GDPR, Access Group redirect the data subject to make its request directly to the data controller, i.e. the school

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Where Access Group have the schools personal data acting in their capacity as data controller, the Access Group will delete the schools personal data in accordance with the Access Group data retention schedule (available via their **Security Portal**), or as otherwise required by data protection legislation: including where the school choose to exercise its rights on behalf of a data subject

  Where Access Group have the schools personal data acting in their capacity as a data processor, Access Group will delete the schools personal data in accordance with the data controller's (the schools) instruction, or as otherwise required by data protection legislation. If Access Group are required by law to retain any of the schools personal data, Access Group will inform the data controller (the school) of this lawful obligation

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Access Group is committed to helping protect the security of the school's information. In compliance with the provisions of Article 32 of the UK GDPR, Access Group has implemented and will maintain and follow appropriate technical and organizational measures intended to protect Customer Data and Support Data against accidental, unauthorized, or unlawful access, disclosure, alteration, loss, or destruction

  Suspected breaches are notified to the service desk, this is logged via Access Group ticketing system, which then goes to the DPO for investigation, the customer are

notified of any suspected breaches discovered internally. The Access Group will work with the school to resolve any data breaches

- **ISSUE:** Data is not backed up
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Mirrored Data centres are located in Northampton and Leeds. Backups – every 30mins, and then nightly, patching is completed by the Access Group hosting team

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The UK has been granted an adequacy decision from the EU, meaning the laws and practices of the UK have been found to offer an essentially equivalent level of protection to personal data as is granted in the EU.
  In the event the adequacy decision is revoked or expires (without renewal) and to ensure continuity of service for Access Group customers, they have incorporated the Standard Contractual Clauses (SCCs) into customer contracts, accessible via Access Group Brexit update (available here).
  The SCCs shall sit silent until and unless they are required to be put in place by either the UK or EU GDPR

- **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 data protection law, data subjects have rights including: Right of access – Data subjects have the right to ask us for copies of your personal information. Right to rectification - Data subjects have the right to ask Access Group to rectify personal information they think is inaccurate. Data subjects also have the right to ask Access Group to complete information which they think is incomplete. Right to erasure - Data subjects have the right to ask Access Group to erase their personal information in certain circumstances. Right to restriction of processing - Data subjects have the right to ask Access Group to restrict the processing of their personal information in certain circumstances. Right to object to processing - Data subjects have the right to object to the processing of their personal information in certain circumstances. Right to data portability - Data subjects have the right to ask that Access Group transfer the personal information they gave us to another organisation, or to the data subject, in certain circumstances

  The Privacy Notice states that to exercise any of these rights, please contact Access.DPO@theaccessgroup.com

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Access Group is the data processor, processing the school's personal data through the use of School Admissions Management. The school as data controller still has ownership of the data

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

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Access Group is committed to helping protect the security of the school's information. In compliance with the provisions of Article 32 of the UK GDPR, Access Group has implemented and will maintain and follow appropriate technical and organizational measures intended to protect Customer Data and Support Data against accidental, unauthorized, or unlawful access, disclosure, alteration, loss, or destruction. Access Group has the following accreditation:

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

  This means that independent auditors have examined the controls protecting the data in Access Group systems (including logical security, privacy, and data centre security), and assured that these controls are in place and operating effectively

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, Certified, Penetration Testing, Cyber essentials and ISO 27001	Reduced	Medium	Yes
Data Breaches	Documented in Access Group Services Terms	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:	**Headteacher**	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	**Headteacher**	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:

Clarification has been sort on the following from Access Group's DPO. The answers have been incorporated in the risk, issues and mitigation log in section 2 of this DPIA:

1. What is the 'upload' process? If through a website portal, how is the data secured in transit between the school and Access Group servers? ie. Does the browser utilise TLS/SSL connections with AES-256bit encryption?
2. Could you please advise what server hosting services and the physical access controls, security of the servers, permission-based access, CCTV recording, Cyber Essentials certification, vulnerability and penetration testing?
3. Where is the data hosted i.e. UK-based data centres?
4. Is any data transferred or shared with partners or third-parties outside of the UK?
5. Should demand unexpectedly increase, can your server hosting service scale their facilities to meet demand?
6. 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?
7. Is school data encrypted at rest on the hosting servers? Who has access to the data and what access controls do you put into place?
8. What is the data breach notification process?
9. Clarification on Access Group's data retention period?

DPO advice accepted or overruled by:

Yes

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:	**Headteacher**	The DPO should also review ongoing compliance with DPIA