Data Protection Impact Assessment (Electronic Visitor Management (EVM) provided by Education & IT Ltd (EdIT))

Old Park School operates a visitor management system called Electronic Visitor Management (EVM), this is provided by Education & IT Ltd (EdIT). As such Old Park School must consider the privacy implications of such a system. The Data Protection Impact Assessment is a systematic process for identifying and addressing privacy issues and considers the future consequences for privacy of a current or proposed action.

Old Park School recognises that moving to an electronic sign in solution has a number of implications. Old Park School recognises the need to have a good overview of its data information flow.

The Data Protection Impact Assessment looks at the wider context of privacy taking into account Data Protection Law and the Human Rights Act. It considers the need for a visitor management system and the impact it may have on individual privacy.

Old Park Schoolneeds to know how and where information is stored. The school will need to be satisfied that as data controller EdIT has taken appropriate security measures in terms of processing personal data, and that the rights of the data subject under UK GDPR is satisfied by the application. Old Park School aims to undertake a review of 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 4

Step 3: Consultation process 9

Step 4: Assess necessity and proportionality 9

Step 5: Identify and assess risks 11

Step 6: Identify measures to reduce risk 12

Step 7: Sign off and record outcomes 13

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 record staff and visitor movements in and out of the school during the day and to ensure that this is done in an effective and efficient way whilst taking into consideration Data Protection Law. Old Park School will undertake the following processes:

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

By opting for EVM by EdIT the school aims to achieve the following:

1. Management of staff, and visitor information in one place
2. Efficiency in speeding up the signing in process
3. Security of information
4. Production of bespoke identity badges
5. Storage of information electronically
6. Good working practice, ability to know who is on site
7. Meeting health and safety, and safeguarding risks

The school used a manual system to log movements of staff and visitors in and out of the school. The school recognises that having a manual record has the potential for third party access to personal data and by purchasing an electronic system this goes some way to mitigate against this risk.

Information is stored directly in the visitor management system and is stored locally and in the Cloud. EdIT have remote access with the school's data.

The schools Privacy Notice has been updated accordingly. EVM is also noted as an information asset in the Old Park School Information Asset Register.

Step 2: Describe the processing

Staff will use the system to sign in and out by entering a personal code.

Visitors will sign in and out and a photo will be taken, information requested will be: -

- Their first name
- Their last name
- Company name (if applicable)
- Contact number
- Vehicle registration (if applicable)
- Who they are visiting

Regular visitors will be set up as a registered visitor with their photo, details of their employer and a personal code for them to sign in with.

The system records arrival and departure times and photos of Visitors and Staff.

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?

What is the source of the data? – When the visitor arrives, they use the sign in screen, where data is collected on the name of the individual, who they are visiting, the organization they represent, and car registration details. A photograph is taken of the individual during the signing in process. This photograph is then produced as a visitor badge and given to the visitor.

Staff information is set up by an administrator drawn from information held on the school's Management Information System.

Will you be sharing data with anyone? – Old Park School will not be sharing this information with anyone else. However, in the event of an incident on school premises, the information may be shared with Senior Leadership Team and the relevant authorities for investigation and enforcement purposes.

EVM has an electronic Privacy Notice which is readable when visitors register. It advises what information is taken as part of the registration process, the lawful basis for processing the information, and the data retention period applied.

What types of processing identified as likely high risk are involved? – All information is held locally and is transferred from the school to the cloud. The data is held securely within EVM with administrator access restricted by password.

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 name of staff and date and time of entry and exit. The data is obtained from the school's management information system.

Contractor, Visitor and Volunteer data captures the name of the person, company, car vehicle registration, the person they are visiting, photograph and time of entry and exit

Governing Body member data relates to name, car registration number, photograph and time of entry and exit.

Special Category data? – Personal data revealing the racial, ethnic origin, and in some cases health by taking photographic images may be stored in EVM.

How much data is collected and used and how often? – Personal data is collected each time staff, visitors, Governing Body members and volunteers come to the school.

How long will you keep the data for? – The school follows the good practice in terms of data retention as set out in the Records Management Society IRMS Toolkit for schools (Visitor Books and Signing in Sheets suggest Current year + 6 Years then review)

Scope of data obtained? – The number of people with their own login are 147 Workforce, 6 Governors, 1 Volunteers 39 Registered visitors from Health, Agencies, Local Authority etc. and 215 former members of staff, Agencies, Local Authority etc.
Registered visitors from Health, Agencies, Local Authority etc. and former members of staff, Agencies, Local Authority etc.

There are also any visitors that sign in to the school. This includes Parents, Supply Agency staff, Contractors and Educational and Health specialists (the number varies).

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. There are a large number of visitors each day to the School.

What is the nature of your relationship with the individuals? – Old Park School collects and processes personal data relating to its employees, visitors, volunteers, and Governing Body Members to accurately monitor who is in school at any one time. This is in line with Safeguarding and Health and safety requirements.

Through the Privacy Notice (Workforce/Volunteer and Governor) Old Park 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 data held on EVM will be controlled by username and password. Access to the system is limited to the Administration Team. The school uses its password policy to ensure these are compliant with information security standards.

Are there prior concerns over this type of processing or security flaws? – The information is stored locally and in the cloud and administrator access to EVM is controlled by password access.

Old Park School recognises that moving from a manual signing in and out system to one which holds personal data electronically raises a number of General Data Protection Regulations issues as follows:

- **ISSUE:** EVM will be storing personal data
  RISK: There is a risk of unauthorized access to information by third parties
  MITIGATING ACTION: The data is housed on the EVM system within the school's premises. The school uses an authentication process using a username and password to the system.

- **ISSUE:** EVM as a third party processor and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: It is advisable that the school tailor any contract to incorporate these privacy commitments. Incorporated within the school's Privacy Notice

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The school will recognize the need to define in their contract a breach event and procedures for notifying the school and the school managing it

- **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: The EVM system has the capability to allow the school to address the rights of the individual. If the school requires assistance for undertaking this type of work the school can contact the EVM Support Team (EdIT)

EVM software provides greater local control of the system and requires less assistance from the support desk and has been developed to reflect the changes that have taken place in data protection

- **ISSUE:** 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
  RISK: The school is unable to exercise the rights of the individual
  MITIGATING ACTION: EVM can provide the technical capability to ensure the school can comply with such requests

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The school maintains ownership of the data. In terms of disclosure EVM will not release the information to any third party unless the request is subject to legal obligation without obtaining the express written authority of the school who provided the information

- **ISSUE:** Lawful basis for processing personal data
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: School has included EVM in its Privacy Notice (Workforce), and (Governors and Volunteers). E.g. lawful basis for processing includes 537A of the Education Act 1996 (schools must maintain attendance records), The Regulatory Reform (Fire Safety) Order 2005 England & Wales (requires an emergency evacuation plan and ensure all those on site are safe and accounted for). The school has a Privacy Statement on EVM to inform users what, and why the information is being obtained. This also notes the retention period

- **ISSUE:** Data retention
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: School can apply appropriate data retention periods in line with the school's data retention policy. Visitor attendance current year + 6 years; Staff attendance current year + 6 years; With the version of the software being run by the school, data can be deleted manually with assistance from the support desk based on a requests as well as any relationship that may exist between the system and the school's

Management Information System, relating to staff. For assistance in undertaking this, please contact the support desk

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Education & IT Ltd is registered with the ICO Registration reference number is Z3575889. They use ISO27001 accredited UK data centres on a private cloud.

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 backup solution will realise the following benefits:

- Management of staff, and visitor information in one place
- Efficiency in speeding up the signing in process
- Security of information
- Production of bespoke identity badges
- Storage of information electronically
- Good working practice, ability to know who is on site
- Meeting health and safety, and safeguarding risks

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 (Workforce, Governors and Volunteers). The lawful basis includes the following:

- Health and Safety at Work Act
- Keeping Children Safe in Education
- 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.

EVM 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
Asset protection and resilience	Possible	Significant	Medium
Storing of personal data	Possible	Significant	Medium
Data Breaches	Possible	Significant	Medium
Subject Access Request	Probable	Significant	Medium
Upholding rights of data subject	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
Asset protection & resilience	Service Level Agreement in place	Reduced	Medium	Yes
Storing of personal data	Use of an authentication process, e.g. using a username and password system	Reduced	Low	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
Upholding rights of data subject	Technical capability to satisfy rights of data subject	Reduced	Low	Yes
Data Retention	Implementing school data retention periods as outlined in the IRMS Information Management Toolkit for Schools (Visitor Books and Signing in Sheets suggest Current year + 6 Years then review)	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	**Name/date**	**Notes**
Measures approved by:	**J Colbourne**	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	**J Colbourne**	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) Does EdIT provide the technical capability to ensure the school can comply with rights of access and subject access requests *(i.e. rights to request access, rectification, erasure or to object to processing?)* Yes

(2) Does the functionality exist to enable the school to apply appropriate data retention periods? *(i.e. the period for which personal data will be stored)* Yes

(3) What certification does EdIT have?, *(e.g. ISO 27001 certified, registered with ICO, etc)*

They are registered with the ICO and are working towards ISO 27001 accreditation.

DPO advice accepted or overruled by:

Yes

If overruled, you must explain your reasons

Consultation responses reviewed by:

Retrospective System adopted September 2016

If your decision departs from individuals' views, you must explain your reasons

Comments:

This DPIA will kept under review by:	J Colbourne	The DPO should also review ongoing compliance with DPIA