Data Protection Impact Assessment

Submitting controller details

Name of controller	Lyngford Park Primary School (RHT)
Subject/title of DPIA	Entrysign (visitor sign in system)
Name of DPO	SSE Schools DPO dposchools@somerset.gov.uk

Step 1: Identify the need for a DPIA

Explain broadly what the 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 pupil, 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.

The school will undertake the following processes:

- Collecting personal data
- Recording and organizing personal data
- Storing personal data
- Copying personal data
- Retrieving personal data
- Deleting personal data

By opting for Entrysign the school aims to achieve the following:

- Management of pupil, 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

The school currently uses a manual system to log movements of pupils, staff, visitors in and out of the school. The school recognizes 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. Entrysign draws on pupil and workforce data as a read and write system, i.e. recognition by name, data of birth, class, etc stored on the school’s Management Information System.

Information is stored directly in the visitor management system and is stored locally. Entrysign cannot do anything with the school’s data. The school’s Privacy Notice has been updated accordingly. Entrysign is also noted as an information asset in the The school’s IInformation Asset Register.

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, Workforce and Governor) for the school provides the legitimate basis of why the school collects data. Specifically, this relates to health and safety and the safeguarding of vulnerable groups.

How will you collect, use, store and delete data?

Entrysign collects information when pupils, the school’s workforce, visitors, volunteers, and Governing Board members sign into and out of the system. The information is retained according to the school’s Data Retention Policy. Entrysign states there may be some occasions where all or some of the information from the school’s Entrysign system would be processed by Entrysign Ltd, all of which involves processing data whilst not on the school’s site or within the school’s network. Information is uploaded to the cloud server which is housed in the UK using SSL/https.

What is the source of the data?

In terms of visitor information this is collected via an online registration process where data is collected on the name of the individual, who they are visiting, the organisation they represent, and car registration details. A photograph is taken of the individual during the signing in process. This photograph is then produced in paper format and given to the visitor. Pupil information is obtained on a read and write basis drawn from information held on the school’s Management Information System. Staff information work on similar principles.

Will you be sharing data with anyone?

The 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. Entrysign 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 not transferred from the school to the cloud. The data is held securely within Entrysign 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?

Pupil data relates to the name of the child, date of birth, and class (read and write). If the child goes off site the parent will record the reason why electronically on Entrysign. This will also be recorded as time of entry and exit. Workforce data relates to name of staff and time of entry and exit. The data is obtained from the school's management information system. Contractor, Visitor and Volunteer data would capture 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 Entrysign.

How much data is collected and used and how often?

Personal data is collected when pupils, 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)

How many individuals are affected (pupils, workforce, governors, volunteers)? And what is the geographical area covered?

Year 1 to Year 6 pupils (number of pupils), workforce (number of workforce), Board of Governors (number of Governors), and Volunteers (number of volunteers), and any other, i.e. contractors, education 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)?*

What is the nature of your relationship with the individuals?

The school collects and processes personal data relating to its pupils, employees, visitors, volunteers, and Governing Body Members to accurately monitor who is in school at any one time. Through the Privacy Notice (Pupil/Workforce/Governor) the 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 Entrysign will be controlled by username and password. The school uses its password policy to ensure these are compliant with information security standards.

Do they include children or other vulnerable groups?

Some of the data will relate to children. This is restricted to their name, date of birth and class.

Are there prior concerns over this type of processing or security flaws?

The information is stored locally and administrator access to Entrysign is controlled by password access

This use of technology is not new or innovative and is common in many schools. There are no issues of public concern.

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:

- Management of pupil, 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

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 the 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 the SSE DPO 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 minimization? 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:

- 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.

How will Entrysign 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** Remote, possible or probable	**Severity of harm** Minimal, significant or severe	**Overall risk** Low, medium or high
1. Asset protection and resilience	Possible	Significant	Medium
2. Storing of personal data	Possible	Significant	Medium
3. Data Breaches	Probable	Significant	Medium
4. Subject Access Request	Probable	Significant	Medium

5. Upholding rights of data subject	Probable	Significant	Medium
6. 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** Eliminated reduced accepted	**Residual risk** Low, medium, high	**Measure approved** Yes / No
1. Asset protection & resilience	Service Level Agreement in place	Reduced	Medium	Y
2. Storing of personal data	Use of an authentication process, e.g. using a username and password system	Reduced	Medium	Y
3. Data Breaches	Documented in contract and owned by school	Reduced	Low	Y
4. Subject Access Request	Technical capability to satisfy data subject access request	Reduced	Low	Y
5. Upholding rights of data subject	Technical capability to satisfy data subject access request	Reduced	Low	Y
6. 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	Y

Step 7: Sign off and record outcomes

<table>
<tr><th>Item</th><th>Name/position/date</th><th>Notes</th></tr>
<tr><td>Measures approved by:</td><td>Helen Morley, HT, Data Protection Lead</td><td>Integrate actions back into project plan, with date and responsibility for completion</td></tr>
<tr><td>Residual risks approved by:</td><td>Helen Morley, Data Protection Lead</td><td>If accepting any residual high risk, consult the ICO before going ahead</td></tr>
<tr><td>DPO advice provided:</td><td>Amy Brittan, SSE DPO</td><td>DPO should advise on compliance, step 6 measures and whether processing can proceed</td></tr>
<tr><td colspan="3">Summary of DPO advice:
• Ensure that privacy notices and Information Asset Register (data asset audit) are updated appropriately.
• Ensure that Entrysign 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.
• Identify the industry certification held by Entrysign (e.g. ISO 27001 certified, registered with ICO, etc)</td></tr>
<tr><td>DPO advice accepted or overruled by:</td><td>Helen Morley</td><td>If overruled, you must explain your reasons</td></tr>
<tr><td colspan="3">Comments:
All of the above checked.</td></tr>
<tr><td>Consultation responses reviewed by:</td><td>Helen Morley</td><td>If your decision departs from individuals’ views, you must explain your reasons</td></tr>
<tr><td colspan="3">Comments:
No other comments or observations</td></tr>
<tr><td>This DPIA will kept under review by:</td><td>Helen Morley.</td><td>The DPO should also review ongoing compliance with DPIA</td></tr>
</table>