Data Protection Impact Assessment (InVentry)

Roberts Primary School operates a visitor management system called InVentry. As such Roberts 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.

Roberts Primary School recognises that moving to an electronic sign in solution has a number of implications. Roberts 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 visitor management system and the impact it may have on individual privacy.

Roberts Primary School needs to know how and where information is stored. The school will need to be satisfied that as data controller InVentry 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.

Roberts Primary 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....13
Step 4: Assess necessity and proportionality....13
Step 5: Identify and assess risks....15
Step 6: Identify measures to reduce risk....16
Step 7: Sign off and record outcomes....17

2

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 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.

Roberts Primary 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 InVentry the school aims to achieve the following:

1. Management of pupil, 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 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.

InVentry 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. InVentry cannot do anything with the school's data.

The schools Privacy Notice has been updated accordingly. InVentry is also noted as an information asset in the Roberts Primary School Information 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? – InVentry 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.

InVentry states there may be some occasions where all or some of the information from the school's InVentry system would be processed by InVentry 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 InVentry Anywhere 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 organization they represent, and car registration details. A photograph is

4

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? – Roberts Primary 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.

InVentry 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 InVentry 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?

5

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 InVentry. 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 InVentry.

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)

Scope of data obtained? – 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

6

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? – Roberts Primary 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) Roberts 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 data held on InVentry 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 InVentry is controlled by password access.

Roberts Primary 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:** InVentry will be storing personal data
  RISK: There is a risk of unauthorized access to information by third parties
  MITIGATING ACTION: All onsite and cloud stored data will be secured using 256-bit AES encryption, this is the responsibility of the processor. The security of the on-

7

premises device e.g. antivirus, firewall, password policy is the responsibility of the data controller

All InVentry staff receive appropriate training and are subject to confidentiality with regards to school data

- **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: InVentry data is hosted on Microsoft Azure servers based in the UK

- **ISSUE**: Transfer of data between the school and the cloud
  RISK: Risk of compromise and unlawful access when personal data is transferred
  MITIGATING ACTION: Transport and storage of all personal data originating from schools using modern and best practice encryption technologies such as Secure Socket Layers (SSL/HTTPS/TLS 1.2) for encrypted data transfer over the internet

8

Any data copied for support calls and incident resolution is done using remote support software which uses RSA private/public key exchange (2048-bit) and AES (256-bit) session encryption

- **ISSUE:** InVentry 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: IInVentry shall, upon confirmation of a data breach notify the data controller of it within 24 hours and will work together with Data Controller to investigate the data breach where this is within its control

  InVentry Ltd shall indemnify the Data Controller against all liability, loss, damage and expense of whatsoever nature incurred or suffered by the Data Controller due to any failure by InVentry Ltd or its employees, agents or Sub-processors to comply with any of its obligations under this agreement and/or under Data Protection Legislation. Similarly, The Data Controller shall indemnify against all liability, loss, damage and expense of whatsoever nature incurred or suffered by InVentry Ltd due to any failure by the Data Controller or its employees or agents to comply with any of its obligations under the agreement and/or Data Protection Legislation

- **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 InVentry 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 InVentry Support Team

9

From Version 4 InVentry 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: InVentry can provide the technical capability to ensure the school can comply with such requests

- **ISSUE:** Third Party Access
  RISK: UK GDPR Non Compliance
  MITIGATING ACTION: If InVentry choose to change a third party service, they will complete an appropriate data protection impact assessment, alter their privacy statement where appropriate and notify the school of this change. Where an additional service is being provided, consent will be sought

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The school maintains ownership of the data. In terms of disclosure InVentry 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 (please see InVentry Privacy Notice)

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: InVentry data is hosted on Microsoft Azure servers based in the UK

- **ISSUE:** Lawful basis for processing personal data
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: School has included InVentry in its Privacy Notice (Pupil), (Workforce), and (Governors and Volunteers). E.g. lawful basis for processing includes 537A of the Education Act 1996 (schools must maintain attendance records), The

10

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 InVentry 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; and pupil attendance date of entry + minimum period of 3 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 request 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:** Data is not backed up
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Data is backed up on an hourly, daily, and weekly basis

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

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: InVentry is registered with the ICO (https://ico.org.uk/ESDWebPages/Entry/Z312861X). InVentry is Cyber Essentials Accredited by Crest - Certificate no.: 9002970002587254

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?

11

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
- Meeting health and safety, and safeguarding risks

12

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 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.

InVentry 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

13

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

14

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

15

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

16

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Dawn Hunt	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Dawn Hunt	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 InVentry 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?)* *(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)* (3) What certification does InVentry have? *(e.g. ISO 27001 certified, registered with ICO, etc.)*		
DPO advice accepted or overruled by: If overruled, you must explain your reasons		
Consultation responses reviewed by: If your decision departs from individuals' views, you must explain your reasons		
Comments:		
This DPIA will kept under review by:	Dawn Hunt / Julie O'Shaughnessy	The DPO should also review ongoing compliance with DPIA

17