

Data Protection Impact Assessment (DPIA)

Guidance for Schools When Completing A DPIA Prior to Implementing BoomReader

Overview

This is a suggested template and should be adapted by schools to fit particular circumstances. Please read the template carefully and consider if what is stated is applicable to your situation. Schools should make amendments to this document where needed.

The completed DPIA should be signed off by the Data Protections Officer and School Governors.

If you identify a high risk to privacy that you cannot mitigate adequately, Data Protection Law requires that you must consult the ICO before starting to process personal data.

This is how the Information Commissioner's Office describes a DPIA:

"A DPIA is a process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of your accountability obligations under the GDPR, and when done properly helps you assess and demonstrate how you comply with all of your data protection obligations.

It does not have to eradicate all risk but should help you minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what you want to achieve.

DPIAs are designed to be a flexible and scalable tool that you can apply to a wide range of sectors and projects. Conducting a DPIA does not have to be complex or time-consuming in every case, but there must be a level of rigour in proportion to the privacy risks arising."

Documents Required

Squirrel Learning Limited (the owners of BoomReader) provide the following supporting documents which are downloadable from the website www.boomreader.co.uk:

- Terms and Conditions
- Privacy Policy
- Data Protection Policy

Introduction

The school wishes to use BoomReader, an online tool/app provided by Squirrel Learning Limited as part of the school approach to literacy. Pupils will have access to this in school, and at home. The purpose is to provide an electronic reading record, aimed to replace paper reading records. The purpose of this data sharing with a third-party provider is to enhance children's learning and to make recording their reading enjoyable, to save the school money (no more paper books to buy) and to enable staff to quickly check which children are recording in their records (rather than flicking through books) which will enable staff to quickly identify where further support is needed.

The BoomReader platform also enables some reading engagement analysis to take place. Staff can see which children are engaging with the tool and identify pupils that may need extra encouragement them to read. This data will be used to supplement teacher tracking of progress and assessment of ability:

Screening Questions

Will the project compel individuals to provide information about themselves? If yes, please detail the information to be provided.

- School name and contact information (including school postal address, phone number and email address)
- Teachers' names and contact information (including phone numbers and email addresses)
- Pupils' names, class/year group
- Parent email addresses (optional).

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? If yes, please detail which organisations will be provided with access.

Yes. The school will be sharing data with an external company who will be a data processor. Data will be shared by creating a csv excel spreadsheet containing the personal data to be uploaded to the platform.

Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition. If yes, please detail the new technology, below.

No.

Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them? If yes, please describe the impact, below.

No.

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private. If yes, please describe the information to be collected, below.

No.

Will the project require you to contact individuals in ways that they may find intrusive? If yes, please describe how the individuals will be contacted, below.

No.

Note regarding Consultation.

We will consult with our DPO and Governors regarding this project. We do not intend to formally consult with parents/carers regarding data protection issues. We do not need to rely on consent as a basis for processing. However, as we will be encouraging parents to access the website (and/or app) to log reading events and add comments, we will consult with them and ensure they are engaged, and any questions are responded to. Parents will also be able to download an app that will allow them to log reading activity- however, they are not compelled to do so.

After completing the above screening questions and identifying simple ways to eliminate any risks to privacy it was decided (upon advice from the DPO) not to complete a full DPIA. However, because the school takes data protection requirement seriously, this document outlines the reasoning behind the decision, an action plan and sets out the terms and conditions and privacy notice of the providers. These have been checked by the DPO.

Reason for this decision:

- The provider will be given the minimum amount of data needed to use the system (pupil name and class only)
- Pupils will log in with a unique class code and their own 5-digit pin number.
- Staff will be asked to keep their passwords safe as per the IT Acceptable Use Policy.
- Pupils/parents provided with logins will only be able to access their own virtual reading record.
- It was felt with these additional security measures in place that any data risk would be classed as low.

Actions to take.

- Obtain approval of DPO and Data Protection Governor.
- Enter into contract with Squirrel Learning Limited for BoomReader (the DPO has checked the Terms and Conditions and Privacy Policy, and these are satisfactory for the purpose)
- Upload information via csv spreadsheet
- Retain pupil data in line with guidance in the retention schedule and delete at the end of the period of retention (consider revising retention policy if it is desired that these records are kept for longer than the current year).
- Keep this document under review and check use of provider is in accordance with the intentions set out in this document.

Appendix A: Evidence of due diligence of supplier

Squirrel Learning Limited,
Technology Centre
University of Wolverhampton Science Park,
Glaiser Drive,
Wolverhampton
West Midlands, WV10 9UR.

ICO Registration: ZA871297

www.boomreader.co.uk

The DPO has read the above documents and they are suitable for the processing operation.

Appendix B: Checking the processing against the Data Protection Principles

Answering these questions during the DPIA process will help you to identify where there is a risk that the project will fail to comply with the GDPR or other relevant legislation, for example the Human Rights Act.

Principle 1

Lawfulness, fairness and transparency of data processing

There must be lawful basis for processing the personal data as follows.

- (a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
- (b) Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- (c) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- (d) Vital interests:** the processing is necessary to protect someone's life.
- (e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- (f) Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. This cannot apply if you are a public authority processing data to perform your official tasks.

| | |
|---|----------------|
| Have you identified the purpose of the project and which lawful basis applies? | Yes |
| Is the processing of the data necessary in terms of GDPR? | Yes |
| How will you tell individuals about the use of their personal data? | Privacy Notice |
| Do you need to amend your privacy notices? | Yes |
| If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn? | n/a |
| If special categories of personal data have been identified have the requirements of GDPR been met? | n/a |
| As the School is subject to the Human Rights Act, you will, where privacy risks are especially high, need to consider: | |
| Will your actions interfere with the right to privacy under Article 8 | n/a |
| Have you identified the social need and aims of the project? | n/a |
| Are your actions a proportionate response to the social need? | n/a |

Principle 2

Personal data shall be obtained only for one or more specified explicit and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

| | |
|---|--|
| Does your project plan cover all of the purposes for processing personal data? | Yes |
| Have you identified potential new purposes as the scope of the project expands? | Yes. DPIA screening will be revisited if necessary |
| Does your Privacy Notice cover all potential uses? | Yes |

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

| | |
|---|---------------------|
| Is the quality of the information good enough for the purposes it is used? | Yes |
| Which personal data could you not use, without compromising the needs of the project? | Minimum being used. |

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

| | |
|---|--------------------------|
| If you are procuring new software, does it allow you to amend data when necessary? | Yes |
| How are you ensuring that personal data obtained from individuals or other organisations is accurate? | Check against school MIS |

Principle 5

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary.

| | |
|---|--|
| What retention periods are suitable for the personal data you will be processing? | As per school retention policy. Pupils will have an account for as long as they are at school, after which it will be deleted. |
| Are you procuring software that will allow you to delete information in line with your retention periods? | Yes |

Principle 6

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

| | |
|--|-----------------------------------|
| Do any new systems provide protection against the security risks you have identified? | Yes |
| What training and instructions are necessary to ensure that staff know how to operate a new system securely? | None Data Protection reminders |

Rights of Data Subjects and Privacy by Design

| | |
|---|-----|
| Will the systems you are putting in place allow you to respond to subject access requests? | Yes |
| Will the system allow compliance with individual rights under GDPR, the right to be informed, the right to rectification and the right to be forgotten? | Yes |
| If the project involves marketing, have you got a procedure for individuals to opt into their information being used for that purpose? | n/a |

Transferring data outside European Economic Area

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

| | |
|---|-----|
| Will the project require you to transfer data outside of the EEA? | No |
| If you will be making transfers, how will you ensure that the data is adequately protected? | n/a |