Bedgrove Infant School

GDPR Data Privacy Impact Statement

Last reviewed and approved: January 2024

Next review date: Spring 2026

Appendices Included:

Definitions and Privacy Impact Statement

Modifications 2024:

No changes. Checked version with TIO latest version 105 V1.02

Privacy Impact Assessment PIA

Introduction

Privacy impact assessments were launched in the UK by the Information Commissioner in December 2007 and mandated by the Cabinet Office for Information and Communication Technology projects following the Data Handling Review of June 2008.

Purpose:

The purpose of this document is to set out the process for completing Privacy Impact assessments to identify any impact on privacy where a new service, upgrade or system is introduced.

Scope:

The procedure is to be followed in the following circumstances:

- Introduction of a new information system to collect and hold personal data.
- Update or revision of a system that might alter the way in which the organisation uses, monitors and reports on personal information.
- Changes to an existing system where additional personal data will be collected, a proposal to collect personal data from a new source or for a new activity.
- Plans to outsource business involving storing and processing personal data.
- Plans to transfer services from on provider to another that include the transfer of information assets.
- Any change to or introduction of new data sharing agreements
- Data sharing initiative where two or more organisations seek to pool or link assets of personal data.
- Any change to access of an information asset that involves an external organisation.
- Changes to legislation, policy or strategies which will impact on privacy through the collection of or the use of information, or through surveillance or other monitoring.

Responsibility

Any person who is responsible for introducing a new or revised service or changes to an existing system, process or information asset is responsible for ensuring the completion of a PIA and therefore must be effectively informed of these procedures.

DPIA Process

A PIA should incorporate the following steps (ICO, 2016)

- Identify the need for a PIA.
- Describe the information flows and data mapping.
- Identify the privacy and related risks.
- Identify and evaluate the privacy solutions.
- Sign off and record the PIA outcomes.
- Integrate the outcomes into the project plan.
- Consult with the internal and external stakeholders as needed throughout the process.

Privacy Impact Assessment – Project Details

This Privacy Impact Assessment must be completed wherever there is a change to an existing process or service, or a new process or information asset is introduced that is likely to involve a new use or significantly changes the way in which personal data is involved.

Project Details:	
PIA Reference Number	
Project Description	
Implementing Organisation/Department	

Project Manager/Information Owners Details:	
Name	
Designation	
Email	
Phone	

Project Overview:	
Proposal Summary	
Purpose of the project	
Key Stakeholders	
Proposed Implementation Date	

Stage 1: Initial screening Questions to identify the need for a DPIA

This section is to be completed Manager or Project Lead responsible for delivering the proposed change/system. The purpose of this section is to assess whether a more complete assessment is required. The screening questions will need to be reviewed by a Data Protection Lead or Data Protection Officer. If yes is the response to any of the questions, then an initial Privacy Impact Assessment must be completed.

SN	Screening Question	Yes/No	Explanation
1.1	Will the project involve the collection of new information about individuals?		
1.2	Will the project compel individuals to provide information about themselves?		
1.3	Will information about individuals be disclosed to or shared with organisations or people who have not previously had access to the information?		
1.4	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?		
1.5	Does the project involve using new technology which might be perceived as being privacy intrusive for example biometrics or facial recognition?		
1.6	Does the project include new software, apps or any other new form or information asset that use personally identifiable information in any way?		
1.7	Will the project result in you making decisions or taking actions against individuals in ways which could have a significant impact on them?		
1.8	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, personally identifiable or sensitive information, or other information that people are likely to consider private? [NB: if health information is involved in any way then the answer to this question is always 'Yes'.]		
1.9	Will the project require you to contact individuals in ways which they may find intrusive including contacting subjects for reasons other than normal educational data collection?		

Answering 'Yes' to any of the questions represent a potential information governance risk that needs to be further analysed to ensure those risks are identified, assessed and mitigated. If any of the answers for the above questions is 'Yes' please complete stage 2.

Stage 2: Initial Privacy Impact Assessment

SN	Questions		Explanation
2.1	Is this a new or changed use of personal information that is already collected?	New/Changed	
2.2	**What data will be collected?** • Name: • DOB: • Age: • Gender: • Address: • Phone number: • Email address: • Location data: • Online identifier: • Other unique number: (UPN etc.) • UPN: • SEN: **Other Data (please state)** **Special category data:** • Racial or ethnic origin • Sexual life • Political opinion • Religious belief • Trade union membership • Physical or mental health or condition • Biometric or genetic data **Criminal Record:** • Commission or alleged commission of an offence • Proceeding for any offence committed or alleged **Details and description or any other data collected:**		
2.3	Can the same outcome be achieved without processing any of the above datasets?		Yes/No
2.4	Is the processing fair, lawful and transparent?		Yes/No
2.5	What is the lawful processing basis for this dataset being processed?		
2.6	If legitimate interest is being used has the means test been completed?		Yes/No/NA
2.7	If consent is the lawful processing basis, is the consent and context it was provided recorded?		Yes/No/NA

2.8	Is the information being used for a different purpose than it was originally collected for?	Yes/No
	If Yes, please list the new purpose(s)	
2.9	If being used for a new purpose, is the new purpose compatible with the original purpose?	Yes/No
2.10	Are other organisations involved in processing (including receipt) of the collected data?	Yes/No *If yes list below*

Name of Organisation	**Contact Person**	**Assurance (i.e.) ISO Certificate, Cyber Essentials**

SN	**Questions**	**Explanation**
2.11	Has the data flow mapping exercise been undertaken?	Yes/No
	Can you please provide a copy of the document or complete section 3.0	
2.12	Does the work involve employing external third-party contractors accessing system/data?	Yes/No
	If yes, please provide a copy of agreement/contract	
2.13	Will the information be collected electronically, on paper or both?	
2.14	Where will the information be stored?	
2.15	Who will have access to the system/data?	
2.16	Is there an ability to audit access to the information?	Yes/No
	If yes, who will have access to audit logs?	
2.17	Does the system involve new links with personal data in other system or have existing links been significantly changed?	Yes/No
2.18	How will the information be kept up to date and checked for accuracy and completeness (Data Quality)?	
2,19	What security and audit measures have been implemented to secure access to a limit use of personally identifiable information? (please select) • User name and password: • Encryption: • Smart Card: • Secure Token: • Restricted access to file servers: • Locked physical secure location:	

	Other security measures, please list.	
2.20	Will any of the information be sent (transferred) off site i.e. outside of the organisation and its computer network?	Yes/No
	If Yes, • Within the organisation in a standalone system: • Outside of the organisation: • Outside of UK: • Outside of the EEA:	
2.21	If being sent outside of the EEA, what safeguards will be in place to ensure the fair and lawful processing of any data. i.e. BCR, SCC, EU-US Privacy Shield	
2.22	Please state the method of data transfer • Non-secure email: • Secure email: • Website access: • External Portable device: • File Transfer protocol (FTP): • Post: • Fax: Other transfer method, please state:	
2.23	Are system level security policies in place for the proposed system? If yes, please provide a copy.	Yes/No
	If No, when will the policy be in place?	
2.24	Is staff training for the new system in place? • Data collection • System usage • Collecting consent • Secure processing	Yes/No/NA Yes/No/NA Yes/No/NA Yes/No/NA
2.25	If this new/revised function/system should stop, are there plans in place for how the information will be retained/archived/transferred or disposed of?	Yes/No
2.26	How will individuals be informed about the proposed uses of their personal data? E.g. Privacy notice. If yes, please provide a copy of the information.	
2.27	Are arrangements in place for the following: • Access to data (SAR)	Yes/No/NA

	- Right to rectification - Right to be forgotten - Right to data portability - Right to notification - Right to object	Yes/No/NA Yes/No/NA Yes/No/NA Yes/No/NA Yes/No/NA
2.28	Do you have a data retention policy defined for the proposed data set collection?	Yes/No/NA
2.30	How would you ensure the secure disposal of the data at the end of the retention period?	

3.0 Data flow details and data mapping

SN	Questions	Details
3.1	How has the data been gathered? (source of data)	
3.2	Who has access to the data and what is the process for gaining access?	
3.3	Is there an audit trail showing when data has been accessed and the type of access?	
3.4	How is data stored and who id responsible for the data?	
3.5	Who will the data be shared with? Justification for sharing	
3.6	How will the data be shared/moved?	

Please provide a data flow map, which is a flow chart/graphical of data flow. This should include:

- Incoming and outgoing data
- Organisations and/or people sending/receiving data
- Storage of data and methods of transfer

Please provide comments relating to your project that demonstrate how it is compliant with the data Protection Act and GDPR OR which legislation provide the basis for this activity OR why Data Protection Act requirements may be set aside. Below are references to previous questions whose answers may contain information needed to complete this section.

Principles	Ref Sec	Comments
Principle 1 (Processed lawfully, fairly and transparent manner in relation to data subjects)	2.1 2.5 2.6 2.7	
Principle 2 (Personal data shall be collected for specified, explicit and legitimate purposes)	2.8 2.9 2.18	
Principle 3 (Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is processed)	2.2 2.3	
Principle 4 (Personal data shall be accurate and, where necessary, kept up to date)	2.19	

Principle 5 (Personal data processed for any purpose or for purposes shall not be kept for longer than is necessary for that purpose or those purposes	2.24 2.30 2.31	
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)	2.10 2.11 2.12 2.13 2.14 2.15 2.16 2.17 2.20 2.23 2.24 2.25	
Individual Rights obligation	2.11 2.27 2.28	
Transfer to Third countries obligation	2.21 2.22 2.23	

4.0 Risk Identification, Agreed Actions and Sign Off Form

Risk Mitigation planning details

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**
Example: Data stored outside the EEA and not covered by EU GDPR or UK GDPR regulations	Remote / possible / probable	Minimal / significant / severe	Low / medium / high

What are the key privacy issues and associated compliance risks?
Privacy Risks
Risk to Individuals

Compliance Risks
School risks

Risk Mitigation planning details

Risk	Proposed Solution (Action plan below)	Approved by

Action plan details

Action	Target completion date	Responsible person

Project sign off section

Privacy Impact Assessment sign off	
PIA reference number	

Sign off area – Project coordinator	
Name	
Job title	
Signature	

Date	

Sign off area – Project lead	
Name	
Job title	
Signature	
Date	

Note: Please feed the above information and action plan into the main project plan, this PIA document should be visited at every milestone of the project to ensure all risks are being assessed and mitigated.

Contact information and review

If you would like to discuss anything in this document, please contact:

Position	Name	Email	Phone
School lead	Karen Herring	**kherring@bedgroveinfant.co.uk**	**01296 481353**
Data Protection Officer	**turn IT on**	**dpo@turniton.co.uk**	01865 597620 (option 3)