Privacy Impact Assessment

DPA and GDPR 2018 compliant – "Privacy by Design strategy"

2020-2021

Next review point- Sept 2021

Document Owner- Nexus Information Governance ICT Lead

Screen, Assess, Plan

nexus Multi Academy Trust

Learning together to be the best we can be

"Learning together; to be the best we can be"

Context

The Information Commissioner has issued this code of practice under section 51 of the Data Protection Act (DPA) in pursuance of his duty to promote good practice. The DPA says good practice includes, but is not limited to, compliance with the requirements of the Act. Conducting a PIA is not a requirement of the Act, but undertaking one will help to ensure that a new project is compliant.

Nexus Trust has adopted best practice as set out by the ICO and requires all new projects that store or share data to be screened and assessed as part of the project planning process.

Although a PIA is not a requirement of the DPA, the GDPR 2018 does require data controllers to conduct a PIA where individuals information is stored electronically.

For further information please see the following links

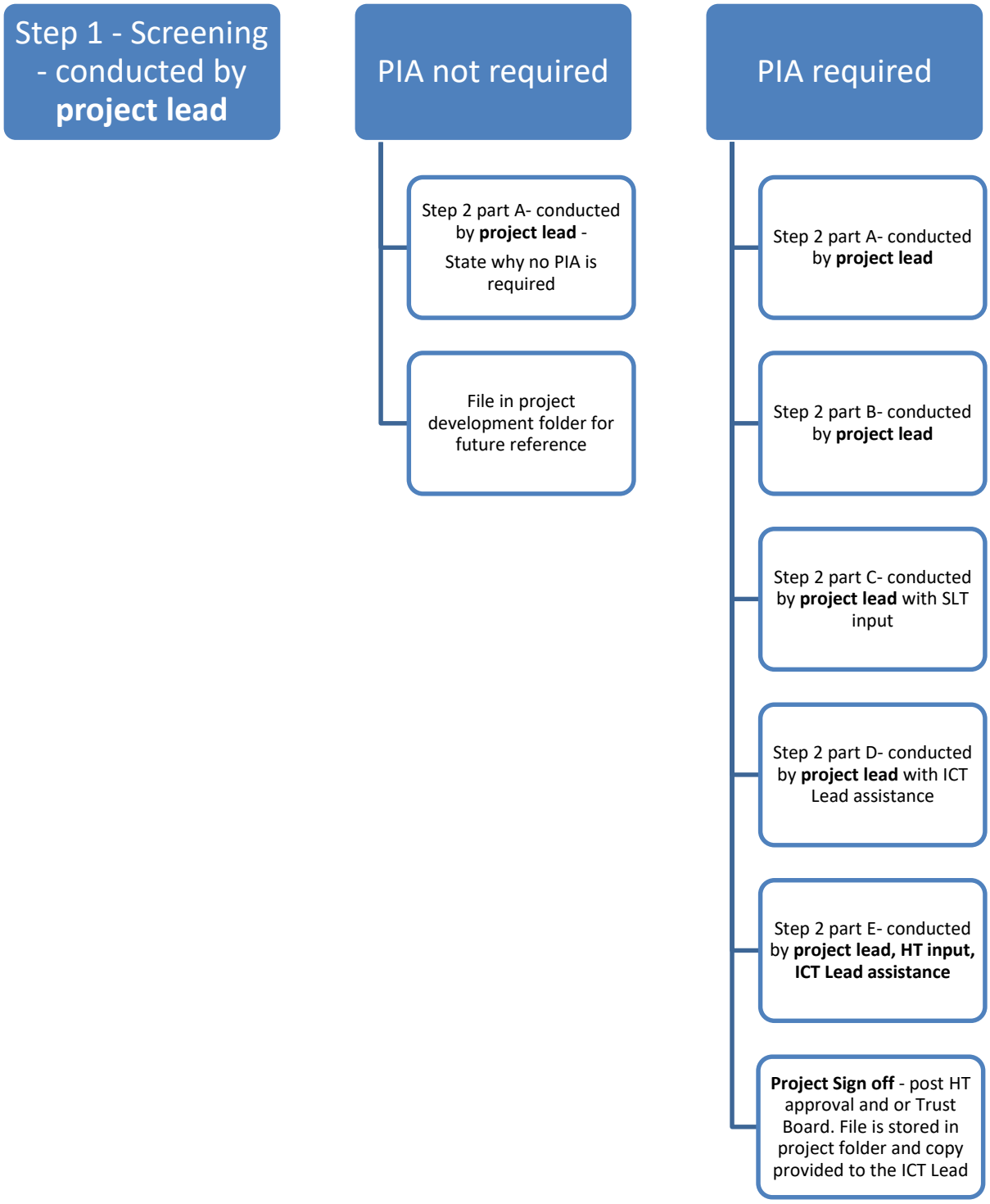
GDPR 2018 - https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

PIA –

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf point 10

The process


Step 1 - Screening - conducted by **project lead**
PIA not required
Step 2 part A- conducted by **project lead** -
State why no PIA is required
File in project development folder for future reference
PIA required
Step 2 part A- conducted by **project lead**
Step 2 part B- conducted by **project lead**
Step 2 part C- conducted by **project lead** with SLT input
Step 2 part D- conducted by **project lead** with ICT Lead assistance
Step 2 part E- conducted by **project lead, HT input, ICT Lead assistance**
Project Sign off - post HT approval and or Trust Board. File is stored in project folder and copy provided to the ICT Lead

Step one - Screening

Please read the questions below and tick the boxes that apply to your project.

- ☐ Will the project involve the collection of new information about individuals?
- ☐ Will the project compel individuals to provide information about themselves?
- ☐ Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
- ☐ Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- ☐ Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, CCTV, the use of biometrics or facial recognition.
- ☐ Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
- ☐ 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 particularly private.
- ☐ Will the project require you to contact individuals in ways which they may find intrusive?
- ☐ Will the information contain personal or sensitive data about students?
- ☐ Will the information contain personal or sensitive data about Staff?
- ☐ Will the information contain personal or sensitive data about third party individuals?

If any of the above questions are ticked, it is advised to complete the PIA process in step 2.

Step 2 – Privacy impact Assessment

Part A – Identify the need for a PIA

[Explain what the project aims will achieve, what the benefits will be to the organisation, to individuals and to other parties.

You may find it helpful to link to other relevant documents related to the project, for example a project proposal.

Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).]

Part B – collection and removal of data

[The collection, usage and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows.
You should also say how many individuals are likely to be affected by the project.
Include any Training aspects, who, how and when.]

Part C – Consultation requirements

[Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process. Consultation can be used at any stage of the PIA process.]

Part D – Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and Corporate risks.
The ICT Lead or CFO/CEO may at this point include any identified risks to the Trust Risk register.

Data type	Data storage and transfer/input type	Risk to individuals	Associated school risk	Corporate risk	Compliance Risk if process not met	Compliance Risk if process met	Risk rating
1.Example – personal	*Cloud based, manual input*	*Identity theft, inaccurate records*	*Financial, public confidence*	*Public confidence*	*High*	*zero*	*low*

Part E – Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary
(e.g. the production of new guidance or future security testing for systems).

Risk	Solution(s)	Result	Evaluation	Managed by	Monitored by
Ref: 1 example	Ensure cloud storage proper levels of security in place, is uk based and encryption is two way for data traffic. Formal Training provided to all staff operators	Certification of security standards provided by company, staff pass training requirements	Third party company to retain security standards annually, Staff level of proficiency is high and maintained	Project Lead and ICT lead	Head teacher

Step 3 – Commission, project Sign-off

The completed assessment should then be provided to the Schools **Data Controller** (Head teacher) and ICT Lead (**Trust Processor**) for commissioning. ***Note*** *- Some projects may need referral to the Trust Board before sign off, these projects would normally require adding to the Trusts risk register.*

Project lead – Print name here…… Date:……..

Signature: ……

ICT Lead – Print name here…… Date:……..

Signature: ……

Head Teacher – Print name here…… Date:……..

Signature: ……

Trust board referred yes/no:…… Date:…… Outcome: ……

Added to the trusts Risk register yes/no: …… Date if applicable: ……