EASTBURY COMMUNITY SCHOOL

DATA PROTECTION IMPACT ASSESSMENT POLICY

If printed, copied or otherwise transferred from the Policies and Procedures Intranet/Internet Site this document must be considered to be an uncontrolled copy.

Policy amendments may occur at any time and you should consult the Policies and Procedures Intranet/Internet Site if in doubt.

Controlled Document

Title	Data Protection Impact Assessment Policy
Document Type	Approved
Author	Data Protection Officer
Owner	Headteacher
Subject	Data Protection Impact Assessment Procedure
Government Security Classification	Official
Document Version	Version 2
Created	August 2019
Approved by	Board of Governors
Review Date	August 2020 or earlier where there is a change in the applicable law affecting this Policy Guidance

Version Control:

Version	Date	Author	Description of Change
1	30/08/2018	Data Protection Enterprise www.dataprotectionenterprise.co.uk	New Policy
2	01/08/2019	Data Protection Enterprise Ltd www.dataprotectionenterprise.co.uk	Annual Review Amendments to: organisation amended to read School

Contents:

1. INTRODUCTION

DOCUMENT STATEMENT AND AIM

This procedure sets out the principles by which Eastbury Community School (hereinafter referred to as the School) will develop, manage, and review the management of Data Protection Impact Assessments (DPIA).

The Information Commissioner's Office defines a Data Protection Impact Assessment (DPIA) as:

'a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. DPIA's help identify privacy risks, foresee problems and bring forward solutions.'

A DPIA is a tool that allows for proper planning for the effective implementation of new or changed systems in a way that assures the confidentiality, security, and integrity of Personal Confidential Data and/or Business sensitive data.

It is as important that a DPIA is carried out when planning changes to processes that handle personal confidential data, as well as when planning the implementation of new systems.

2. SCOPE

This procedure applies to all staff and all processes that include a new or changed use of Personal Confidential Data and/or Business sensitive data in any format.

Typical examples are:

- introduction of a new paper or electronic information system to collect and hold personal/business sensitive data;
- introduction of new service or a change to existing process, which may impact on an existing information system.
- update or revision of a key system that might alter the way in which the School uses, monitors, and reports personal/business sensitive information.
- replacement of an existing data system with new software
- changes to an existing system where additional personal/business sensitive data will be collected
- proposal to collect personal data from a new source or for a new activity
- plans to outsource business processes involving storing and processing personal/ business sensitive data
- plans to transfer services from one provider to another that include the transfer of information assets
- any change to or introduction of new data sharing agreements

3. EQUALITY AND HUMAN RIGHTS STATEMENT

Promoting equality, eliminating unfairness and unlawful discrimination, and treating colleagues, partners and the public with dignity and respect, are fundamental to successful performance by all staff in the School, who are all expected to actively promote equality and

human rights and challenge racism, homophobia, and other forms of discrimination through their activities, and support others to do the same.

All staff are expected to work with others on effective approaches to ensure strategies, policies and activities, promote and demonstrate equality and human rights.

Equality Impact Assessment and Equality Analysis are to be used as part of developing and monitoring proposals and projects for their impact on equality and equity.

All staff, including the Governors are required to abide by all equality and human rights legislation and good practice, and will receive appropriate training and support to do so.

4. ROLES AND RESPONSIBILITIES

4.1 HEAD TEACHER AND SCHOOL GOVERNORS

The Headteacher is responsible for ensuring that DPIA's are carried out for all new or changed uses of Personal Confidential Data as stated above and must sign off each DPIA.

4.2 BUSINESS MANAGERS AND INFORMATION ASSET OWNERS

The Business Manager and Information Asset Owners are responsible for ensuring that new projects or changed ways of working include a DPIA in line with the policy and law noted below.

4.3 STAFF

All staff working in a new or changed way of working with Personal Confidential Data shall ensure that a DPIA is completed following the appropriate process outlined in the flow chart below.

5. GOVERNANCE ARRANGEMENTS

OVERSIGHT

The Oversight of this procedure is with the Data Protection Officer where Information Governance is reviewed, along with the DPIA log and any associated documentation including questionnaires and reports. The Data Protection Officer will receive the questionnaires and DPIAs as necessary to the new or changed use of Personal Confidential Data and provide recommendations as necessary prior to approval by the Headteacher.

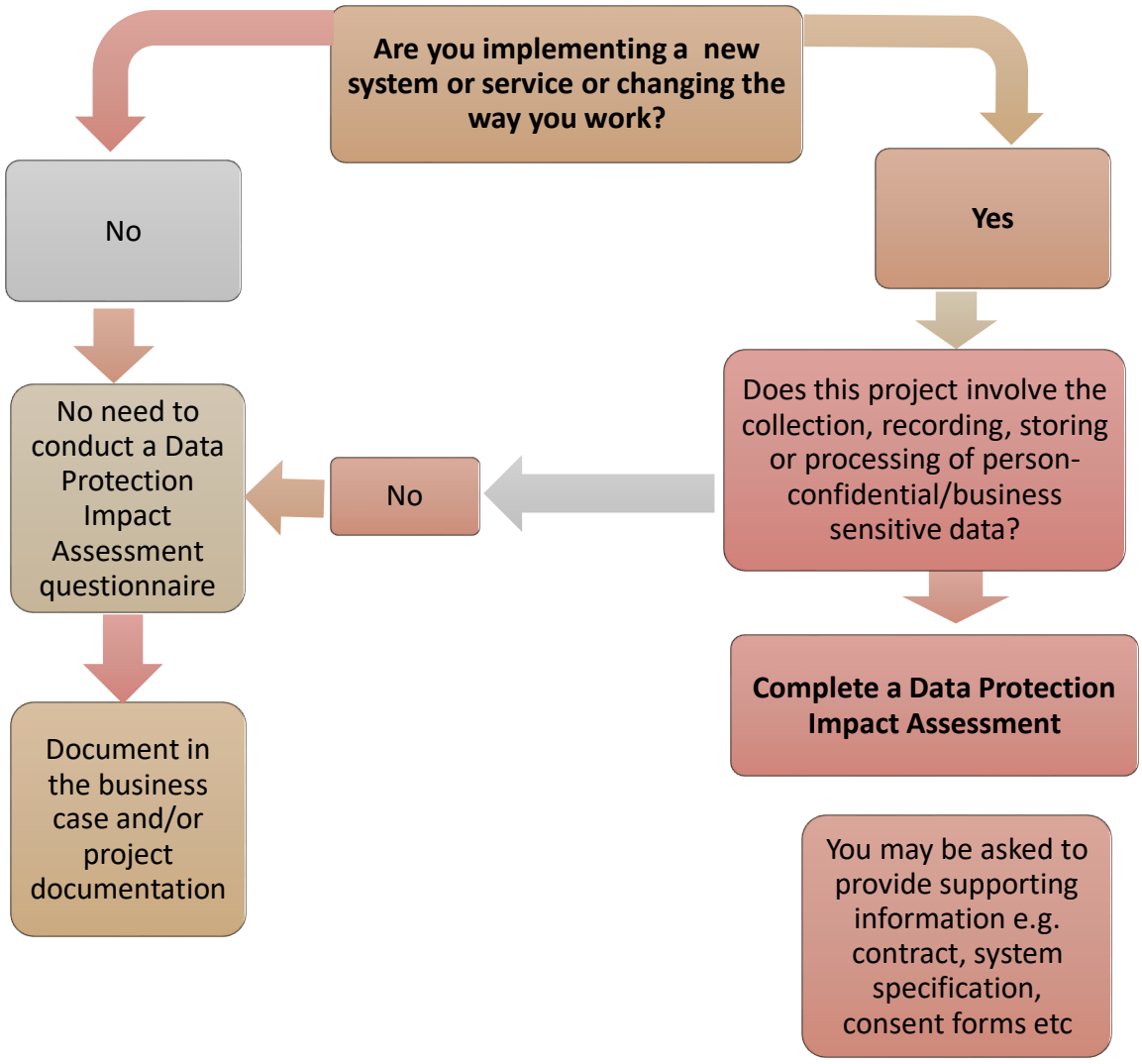
6. PRINCIPLES OF APPLICATION

6.1 IMPLEMENTATION

Prior to the start of a new or changed use of Personal Confidential Information, the responsible person must complete a DPIA questionnaire, which allows for the risk assessment of the project to take place before costs are incurred and for any information risk to be monitored throughout the project.

The following flow chart shows the questions to be answered to determine whether a DPIA questionnaire is required. Where a DPIA questionnaire is identified as NOT being required, this must be documented in the business case and/or project documentation of the new or changed system/process.

Does this project involve the collection, recording, storing or processing of person-confidential/ business sensitive data?

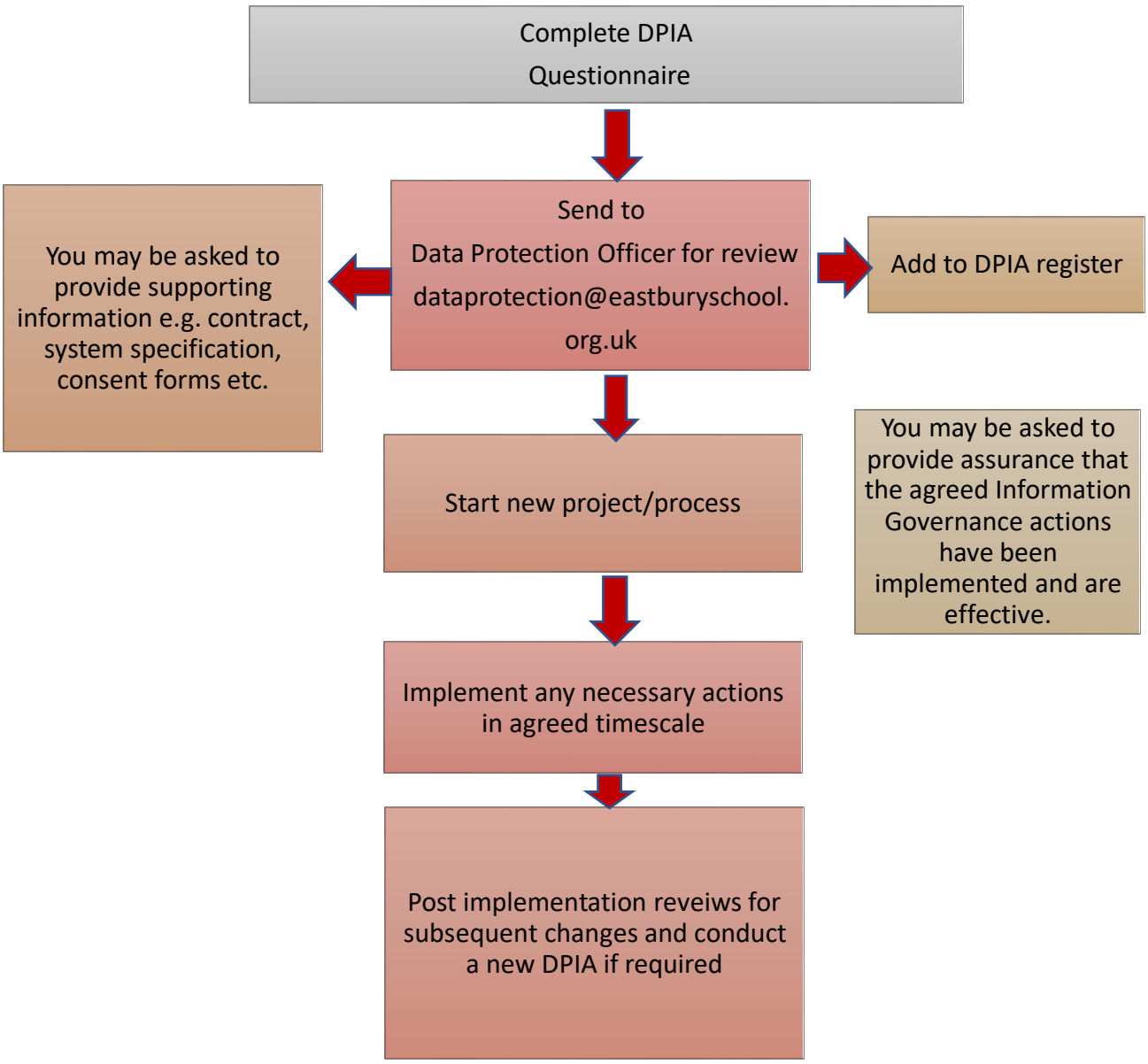


When deciding whether a DPIA questionnaire is required, if the first answer is 'yes', but the second response is 'unsure', please complete the questions in section 1 of the DPIA questionnaire to assist the decision.

If a full DPIA is required where the new process or change of use of Personal Confidential Data/Business Sensitive data, then the completed DPIA must be sent to the Data Protection Officer for review.

6.2 THE DPIA PROCESS

The DPIA process can be displayed as the process diagram below. All stages of the process must be followed in order to ensure proper use of Personal Confidential Data/Business sensitive data.



6.3 STAKEHOLDER ENGAGEMENT

Engagement with key stakeholders throughout the DPIA process ensures all parties are aware of, and will approve, access to Personal Confidential Data without delaying the project. Good communication leads to better understanding of any information sharing and security issues. The DPIA process has the added advantage of propagating a common understanding of the principles and basis for using and sharing Personal Confidential Data/Business sensitive data lawfully and ethically, helping the project to run more smoothly. In some projects, the DPIA can be complicated. In these cases, further guidance should be sought from the Data Protection Officer.

If a high risk is identified that cannot be mitigated, then the Data Protection Officer will consult with the ICO before starting the processing. The ICO will give written advice within eight weeks, or 14 weeks in complex cases.

6.4 DETERMINE

Members of staff should establish and document:

- The purpose of processing the data
- Who are the Data Controllers (sole, joint or in common) and Data Processors (see below for details)
- The legal basis for sharing the information, i.e. consent or another legal basis

The information types (data fields and classes), how the data will flow and where it will be held, what the risks are to its security when in transit and at rest, and what will happen to it once the purpose has been achieved (the information lifecycle)

6.5 DESIGN

Once the determination stage is complete and all the relevant information is collated, the design stage incorporates the following:

- Security standards governing the shared information, and who will be responsible
- System operation
- Stakeholder/End User materials

Care should be taken to ensure that information is handled in accordance with the School policy and within the bounds of the relevant laws. The GDPR has 6 Principles to be adhered to.

6.6 DEPLOYMENT

Physical sharing or 'go live' of the data sharing or new procedure can only take place once the first two sections are complete and signed off by the relevant stakeholders. A DPIA report should be created to collate the steps taken in creating the safe environment for the information to be shared.

7. POLICY AUDIT AND MONITORING COMPLIANCE

POLICY REVIEW

The Data Protection Impact Assessment Procedure will be reviewed annually.

8. STATEMENT OF EVIDENCE/REFERENCES

The legislation and national guidance relevant to this procedure:

- Data Protection Act 2018
- The General Data Protection Regulation 2016/679
- ICO Guidance for Privacy Impact Assessments
- Information Sharing Policy

9. IMPLEMENTATION AND DISSEMINATION OF DOCUMENT

Following ratification, the Data Protection Impact Assessment Procedure will be:

- uploaded onto the School intranet and the document location confirmed to all staff
- the Data Protection Officer will provide training sessions where necessary

10. APPENDICES

Annex 1	Privacy Impact Assessment Screening Questions
Annex 2	Privacy Impact Assessment Questionnaire
Annex 3	Equality and Equity Impact Assessment

Annex one

Privacy impact assessment screening questions

These questions are intended to help you decide whether a DPIA is necessary. Answering 'yes' to any of these questions is an indication that a DPIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

You can adapt these questions to develop a screening method that fits more closely with the types of project you are likely to assess.

Will the project involve the collection of new information about individuals?	Yes	No
Will the project compel individuals to provide information about themselves?	Yes	No
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Yes	No
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	Yes	No
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.**	Yes	No
Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	Yes	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.**	Yes	No
Will the project require you to contact individuals in ways that they may find intrusive?	Yes	No

Annex two

Privacy impact assessment template

This template is to be used to record the DPIA process and results. You should start to fill in details from the beginning of the project, after the screening questions have identified the need for a DPIA.

Step one: Identify the need for a DPIA

Explain what the project aims to 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 DPIA was identified (this can draw on your answers to the screening questions).

Step two: Describe the information flows

Describe the collection, use and deletion of personal data 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.

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.

You can use consultation at any stage of the DPIA process.

Step three: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale DPIAs might record this information on a more formal risk register.

Annex three can be used to help you identify the DPA related compliance risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk

Step four: Identify privacy solutions

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

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Step five: Sign off and record the DPIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by

Step six: Integrate the DPIA outcomes back into the project plan

Who is responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action

Contact point for future privacy concerns

Annex three
Linking the DPIA to the GDPR 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.

Article 5 Principle 1

Personal data shall be processed fairly, lawfully and in a transparent manner

Have you identified the purpose of the project?

How will you tell individuals about the use of their personal data?

Do you need to amend your privacy notices?

Have you established which conditions for processing apply?

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?

If your organisation is subject to the Human Rights Act, you also need to consider:

Will your actions interfere with the right to privacy under Article 8?

Have you identified the social need and aims of the project?

Are your actions a proportionate response to the social need?

Article 5 Principle 2

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Does your project plan cover all of the purposes for processing personal data?

Have you identified potential new purposes as the scope of the project expands?

Article 5 Principle 3

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Is the quality of the information good enough for the purposes it is used?

Which personal data could you not use, without compromising the needs of the project?

Article 5 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?

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Article 5 Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to the implementation of appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

What retention periods are suitable for the personal data you will be processing?

Are you procuring software that will allow you to delete information in line with your retention periods?

Article 5 Principle 6

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Will the systems you are putting in place allow you to respond to subject access requests more easily?

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

Do any new systems provide protection against the security risks you have identified?

What training and instructions are necessary to ensure that staff know how to operate a new system securely?