DATA PROTECTION IMPACT ASSESSMENT POLICY

Date	**September 2020**
Prepared by	**DPO**
Review Date	**September 2021**
Version	**V2**

Date	**September 2019**
Prepared by	**DPO**
Review Date	**September 2020**
Version	**V1**

Introduction

The Rose Learning Trust is committed to promoting best practice in respect of data security and compliance with the General Data Protection Regulations (**GDPR**). Part of our approach is to not only maintain compliance with GDPR, but to also keep your data safe by undertaking a Data Privacy Impact Assessment (D**PIA**).

Purpose

The purpose of this document is to set out the process for completing Data Privacy Impact Assessments (DPIA) to identify any impact on privacy where a new service or system is introduced.

Scope

This 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 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 transfer services from one 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 sets of personal data
- Any change to access of an information asset that involves an external organisation
- Changes in legislation, policy or strategies which will impact on privacy through the collection of or 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 DPIA and therefore must be effectively informed of these procedures

What is a Data Privacy Impact Assessment?

A DPIA is a process that assists organisations in identifying and minimising the privacy risk of new projects or policies. Projects of all sizes could impact on personal data.

The DPIA will help to ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly,

Why should we carry out a DPIA?

Carrying out an effective DPIA should benefit the people affected by the project and also the organisation carrying out the project.

Whilst it is not a legal requirement, it is often the most effective way to demonstrate to the Information Commissioner's Office (ICO) how personal data processing complies with GDPR

A project which has been subject to a DPIA should be less privacy intrusive and therefore less likely to affect individuals in a negative way.

A DPIA should improve transparency and make it easier for individuals to understand how and why their information is being used.

When should you carry out a DPIA?

The core principles of DPIA can be applied to any project that involves the use of personal data, or to any other activity that could have an impact on the privacy of individuals

What do we mean by privacy?

Privacy, in its broadest sense, is about the right of an individual to be let alone. It can take two main forms, and these can be subject to different types of intrusion:

- Physical privacy - the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information
- Informational privacy – the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages

Privacy risk is the risk of harm arising through an intrusion into privacy. This code is concerned primarily with minimising the risk of informational privacy - the risk of harm through use or misuse of personal information. Some of the ways this risk can arise is through personal information being:

- inaccurate, insufficient or out of date
- excessive or irrelevant
- kept for too long
- disclosed to those who the person it is about does not want to have it
- used in ways that are unacceptable to or unexpected by the person it is about
- not kept securely

DPIA Process

A DPIA should incorporate the following step: -

- Identify the need for DPIA

- Describe the information flow
- Identify the privacy and related risks
- Identify and evaluate the privacy solutions
- Sign off and record the DPIA outcomes
- Integrate the outcomes into the project plan
- Consult with internal and external stakeholders as needed throughout the process

Data Privacy Impact Assessment – Please see Appendix 1

APPENDIX 1

This Data 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 significant changes in the way in which personal data is handled

DPIA Project Description	
School	
Project Manager's Details	
Name	
Designation	
Email	
Phone	
Project Overview	
Proposal Summary	
Purpose of the Project	
Key Stakeholders	
Proposed Implementation Date	

Stage 1

The Initial Screening Questions to identify the need for a DPIA

This section is to be completed by the Project Lead responsible for delivering the proposed change/system. The purpose of this section is to assess whether a more complete assessment is required. If response to any of the questions in the screening question is 'YES' than an Initial Data Privacy Impact Assessment must be completed

Please ensure that answers to all questions in each stage of this form are evidenced by providing detailed remarks, and are not simply Yes/No

	Screening Questions	**Yes/No**
1	Will the project involve the collection of new information about individuals?	
2	Will the project compel individuals to provide information about themselves?	
3	Will information about individuals be disclosed to or shared with organisations or people who have not previously had routine access to the information?	
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?	
5	Does the project involve using new technology which might be perceived as being privacy intruding for example, biometrics or facial recognition?	
6	Does the project include new software, apps or any other new form of information asset that use personal identifiable information in any way?	
7	Will the project result in you making decisions or taking action against individuals in ways which could have a significant impact on them?	
8	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records, or their information that people are likely to consider private? (NB if health information is in any way involved, the answer to this question is always 'Yes')	
9	Will the project require you to contact individuals in ways which they may find intrusive?	
10	The project involves making changes to the way personal information is obtained, recorded, transmitted, deleted, or held	

If any of these statements apply to your project, it is an indication that a DPIA would be a useful exercise, and you should complete the rest of the assessment, including the Data Protection Impact Assessment Statement

Stage 2 – - Identifying the Need for a DPIA

Briefly explain what the project aims to achieve, what the benefits will be to the Trust/Academy, to individuals, and to other parties Link any relevant documents i.e. specifications or plans Link back to screening as to reasons why a DPIA is/is not needed

Section 3 – Describe the Information flow

Who will the data be shared with? Justification for sharing How long will the data be retained? – link to Data Retention policy How will the data be destroyed? E.g. physical files will be shredded and confidential wasted Who (and how many) will be affected by the project?

Section 4 – Identifying the Privacy Risks

Answering the questions below will help identify the key privacy risks and the associated compliance and corporate risks

The questions cover the key data protection principles, and whilst all may not be relevant to your project, they may prompt you to consider areas of risk which are not initially apparent

Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. The DPO/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*

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 has 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/DPO and Information Security Consultant*	*Head teacher*

Risk	Solution(s)	Result	Evaluation	Managed by	Monitored by

Principle 1

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject

What personal data will be collected and/or shared?

With whom will the personal data be shared?

How will individuals be told about the use of their personal data?

Conditions for processing - For all data (tick that apply)

The data subject has given consent to the processing	
The processing is necessary for the performance of the contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract	
The processing is necessary for compliance with a legal obligation to which the Trust is subject	

Does your project involve the process of the following?

Data revealing racial or ethnic origin	
Political opinions	
Religious or philosophical beliefs	
Trade Union membership	
Genetic data or biometric data for the purpose of uniquely identifying a natural person	
Data concerning health	
Data concerning a natural person's sec life or sexual orientation	

If so, which of the following apply?

The data subject has given explicit consent to the processing	
The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of The Rose Learning Trust or of the data subject in the field of employment and social security protection law	
The processing is necessary for the establishment, exercise, or defence f legal claims, or whenever courts are acting in their judicial capacity	
The processing is necessary for reasons of substantial public interest	
The processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services	
The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes	

If you are relying on consent to process data, how will this be collected and recorded?

What will you do if consent is withheld or withdrawn? How will this be recorded?

Can an alternative condition for processing be used instead of consent? If yes, please provide details

How will individuals be information at the point of collection about how their personal data will be used?

Will any personal data be published on the Internet or in other media? If yes, please provide details.

Will a third-party contractor be processing the personal data on our behalf, or involved at any stage in the data processing process?

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.

Do you envisage using the personal data for any other purpose in the future? If so, please provide details.

Principle 3 - Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

Are you satisfied that the personal data processed is of good enough quality for the purposes proposed? If not, why not?

Is there any personal data that you could not use, without compromising the needs of the project? If yes, please provide details.

How will you ensure that only personal data that is adequate, relevant, and not excessive in relation to the purpose for which it is processed?

Principle 4 - Personal data shall be accurate and, where necessary, kept up to date.

Are you able to update and amend personal data when necessary, after it has been collected and recorded? Please provide details

How will you ensure that personal data obtained from individuals or other organisations is accurate?

Principle 5 - Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

What retention periods are suitable for the personal data you will be processing? (Link to Data Retention Policy)

How will you ensure the personal data is deleted in line with your retention periods?

What processes will be put in place for the destruction of the personal data?

Principle 6 - Personal data shall be processed in accordance with the rights of data subjects under this Act.

If an individual requested a copy of the personal data held about them, detail how this would be provided to them

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

Principle 7 - 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.

Where, and in what format, will the personal data be kept?

Will an IT system or application be used to process the personal data? Please provide details.

How will this system provide protection against security risks to the personal data?

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

Will staff ever process the personal data away from the office (e.g. via paper files, on laptops, tablets, or smart phones)? If so, please provide details.

How will access to the personal data be controlled?

Principle 8 - Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country of territory ensures and 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 personal data outside of the EEA? If yes, please provide details.

If you will be making transfers, how will you ensure that the personal data is adequately protected

If a contractor is being used to process the personal data, where are they (and their data stores) based?

Data Protection Impact Assessment Statement

This statement must be completed for all projects, regardless of whether a DPIA was deemed to be necessary on completion of the screening questions in Section 1

Note: *some projects may need referral to the Trust Board before signing off. These projects would normally require adding to the Trusts risk register.*

- Please choose one of the following options: - None of the screening statements in Section 1 of this document apply to the above project, and I have determined that it is not necessary to conduct a Data Protection Impact Assessment.
- Some of the screening statements in Section 1 of this document apply to the above project, and a need to carry out a Data Protection Impact Assessment was identified. The assessment has been carried out, and the outcomes will be integrated into the project plan to be developed and implemented

Project lead:	Print name here:	Date:.....
	Signature:	
DPO:	Print name here:	Date:.....
	Signature:	
Head teacher:	Print name here:	Date:.....
	Signature:	

Trust board referred:	Yes/No:	Date:	Outcome: .....
Added to the Trusts Risks register	Yes/No:	Date if applicable:	