Cathedral Schools Trust

Data Protection Impact Assessment Policy and Procedure

It is the responsibility of all Cathedral Schools Trust employees and volunteers to familiarise themselves with the contents of all Trust policies and any amendments hereafter.
Please note that Trust includes all schools and related parties within Cathedral Schools Trust

Throughout this document reference to the "Trust" means Cathedral Schools Trust (CST) and each academy/free school, "Trust Board" means the board of trustees of CST and "parents" means parents and/or carers.

Changes

Version	Date	Amended by	Recipients	Purpose
1	30 September 2021	CST Trustees	Members of CST, every Trustee, each Local Governor, all Cathedral Schools Trust employees and volunteers and others at the discretion of the Chairman of the Trustees of CST. CST Website updated.	Drafted and Updated following Brexit transition and introduction of UK GDPR.
2				
3				

Alterations

This Policy may be altered, added to or repealed by a majority resolution of the Trustees of CST in a general meeting.

Approvals (Every two years)

Version	Date	Approved by
1	30 September 2021	CST Trustees
2		
3		
4		

Table of Contents

1. Definitions

Initiative - any initiative considering change, for example a new policy, process, procedure, project, IT system or procurement activity.

Privacy – in its broadest sense the right of an individual to be left 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. For example, intrusion can come in the form of unwelcome searches of a person's home or acts of surveillance and the taking of biometric information.
- **Information 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. For example intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of information.

Data Protection Impact Assessment (DPIA) – a process which assists the Trust in identifying, minimising and addressing the privacy risks associated with any new initiative.

Advice sought and consultation – activity to allow people to highlight privacy risks and solutions based on their own areas of expertise. This can include seeking advice from internal stakeholders or formal consultation with external stakeholders including partners or service users

Information Asset – is current information held by the organisation which is categorised from the perspective of its content/ business use rather than necessarily an IT system. It could be a collection of paper or electronic records held by the Trust that contain customer/ service user, stakeholder, staff or pupil data. The data the asset holds must be personal and/ or sensitive

Personal data - is information about a person which would enable that person's identity to be established. Sensitive data is anything which if lost or compromised could affect individuals, organisations or the wider community. Sensitive data is defined by the UK General Data Protection Regulation as including:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- health data;
- genetic data;
- biometric data for the purpose of uniquely identifying a natural person;
- data concerning a natural person's sex life or sexual orientation.

---

2. Background information

Completion of a Data Protection Impact Assessment (DPIA) is a requirement of Article 35 of the UK General Data Protection Regulation

With so much information being collected, used and shared in our Trust, it is important that steps are taken to protect the privacy of each individual and ensure that personal information is handled legally, securely, efficiently and effectively.

Completion of a DPIA will assist us to identify and minimise our privacy risks to comply with our data protection obligations and meet individuals' expectations of privacy.

3. The scope of the policy

The policy covers any initiative considering change, for example a new policy, process, procedure, project, IT system or procurement activity. For the purposes of this policy ‘initiative’ will cover all of the activity listed above.

The policy provides a process which will enable:

- identification of the need to complete a DPIA through a set of screening questions;
- the collection of sufficient information about an initiative to complete a DPIA;
- privacy risks identified by the DPIA to be documented and considered;

The process should be followed from the start of an initiative to ensure that potential problems are identified at an early stage, when addressing them will be simpler and less costly and the direction of work can be influenced.

Although the policy is aimed at new initiatives, information asset owners may wish to use it as a tool to review existing arrangements to identify and address privacy risks as a continuous improvement activity.

4. Duties and responsibilities

The Trustees have overall responsibility for the strategic direction and governance of the Trust, including ensuring that Trust processes comply with all legal, statutory and good practice guidance requirements.

The Executive Principal is responsible to theTrustees for ensuring the Information Security Assurance and Risk Management Plan is implemented and reviewed and its effect monitored. The DPIA is one element of the management of information risk. Information risk needs to be handled in a similar manner to other major risks such as financial, legal and reputational risks.

General staff responsibilities – all Trust staff must follow the requirements of this and related policies particularly those relating to information governance. Particular care should be taken of the privacy impact of working with contractors and partner organisations.

5. The benefits of a DPIA

The completion of a DPIA is a requirement under UK GDPR and, as such, the ICO may ask an organisation to view a DPIA. It is an effective way to demonstrate to the ICO how personal data processing complies with the UK GDPR.

We can increase pupil, parent and employee confidence in the way we will use their information. An initiative 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 will demonstrate transparency and may make it easier to explain to individuals why their information is being used.

It will support our legal obligations under the UK GDPR.

Completing a DPIA in the early stages of an initiative will ensure privacy issues are identified early on and most importantly inappropriate solutions are not implemented that later have to be reversed.

Carrying out a DPIA should benefit the Trust through better policies and systems being produced and improving relationships with individuals.

---

6. The DPIA process – key points

The DPIA process is flexible and can be integrated within our existing approach to managing initiatives including those managed through project management arrangements. Appendix C details an overview of the process. The time and resources dedicated to a DPIA should be scaled to fit the nature of the initiative.

A DPIA should begin early in the life of an initiative and should continue to be considered through to implementation.

The DPIA incorporates the following steps:

- identify the need for a DPIA;
- describe the information flows;
- identify the privacy and related risks;
- identify and evaluate the privacy solutions;
- sign off and record the DPIA outcomes;
- integrate the outcomes into the key documentation;
- consult with internal and external stakeholders as needed throughout the process.

---

7. Guidance for completion of a DPIA

When do I need to complete a DPIA?
You should complete a DPIA at the start of any initiative and use it to maintain awareness and regularly review privacy risks through to completion of work. For procurement activity the DPIA should be completed prior to tender to ensure all relevant privacy risks are considered when preparing specifications.

Who should identify the need for a DPIA and complete it?
It is the responsibility of the lead of an initiative to identify the need for a DPIA and complete it. This may be a process owner, manager of the service area completing the initiative or in the case of formal projects the service lead.

How to identify the need for a DPIA?
The consideration of a number of screening questions will identify the need to complete a DPIA. If any screening question is answered ‘yes’ a DPIA will need to be completed. The screening questions are detailed in a template attached at appendix C.

How do I complete a DPIA?
The template attached at appendix C will guide staff through the completion of a DPIA.

Why do I need to describe the information flow in a DPIA?
Understanding the information flows involved in an initiative is essential to a proper assessment of privacy risks. Existing processes and resources such as information audits and the information asset

register can be a useful tool in completing this step of a DPIA. The DPIA template (step two) highlights important information to consider in describing an information flow.

How do I identify a privacy issue and evaluate a solution?
When conducting a DPIA it is necessary to identify any privacy risks and their potential consequences for individuals, compliance and for the Trust such as fines for noncompliance with legislation or reputational damage leading to loss of trust. The DPIA template (step three) provides a table to record the privacy risks and their consequences. Appendix A provides information about potential privacy risks. The following may also provide useful information:

The ICO's Anonymisation: Managing Data Protection Risk Code of Practice may help to identify privacy risks associated with the use of anonymised personal data.

The ICO's Data Sharing Code of Practice may help to identify privacy risks associated with sharing personal data with other organisations.

The ICO's codes of practice on privacy notices and CCTV, as well as other more specific guidance, will also help to focus DPIAs on those issues.

The DPIA template (step four) provides an optional table to score the level of risk for each privacy risk identified and to evaluate the solution/s identified by measuring the inherent risk score. Any privacy risk with a residual score of 6 or more should be regarded as high risk by the Trust. It is the responsibility of the Trust to record relevant risks in the appropriate risk register.

Why do I need to sign off and record the DPIA outcomes?
A key part of the DPIA process is deciding which privacy risks to take forward and recording whether the risks that have been identified are to be tolerated (accepted), treated (reduced), eliminated or transferred. It may be decided that an identified risk is tolerated. However, if there are unacceptable privacy risks which cannot be treated, eliminated or transferred then it will be necessary to reassess the viability of the initiative or a proposal of that initiative. You must record details of the decision maker, who has signed off each risk and the reasons behind their decision.

Who do I need to consult/ seek advice from?
Consultation and seeking advice is an important part of the DPIA process (and can happen at any stage) allowing people to highlight privacy risks and solutions based on their own areas of expertise. Internal activity will be with a range of internal stakeholders for example Governors, Legal, HR, or IT (this list is not exhaustive and you need to establish the key internal stakeholders to your initiative). It may take the form of a written communication/ document or verbal discussion taking place in a focus group or project team meeting. External activity provides an opportunity to gain input from people who could be adversely affected by the initiative if privacy risks are not properly considered and addressed. This may take the form of but not limited to electronic consultation or focus groups for service users. The decision to conduct external consultation may be decided as part of the solution to a privacy risk identified.

What documents should be updated?
The DPIA process should be integrated into existing process documents used to plan work required for the initiative. In the case of formal projects this includes the project initiation document (PiD), plan, action/decision, risk/issue log, comms/ consultation plan and the equality impact assessment (if appropriate). The Information Asset Register must be updated for any changes made to information assets. Decision reports should include reference to the privacy risks and mitigation identified.

What do I do with completed screening questions and DPIAs?
A copy of the completed screening questions and DPIA should be retained within the Information Asset Register (or Records of Processing Activity) electronic folders for future reference.

How do I report an identified risk?
A key principle of DPIA is that the process is a form of risk management. When carrying out a DPIA you should identify any privacy risks to individuals, compliance risks and any related risks for the Trust; such as fines for non-compliance with legislation or reputational damage leading to loss of business. (Appendix A refers to possible risks you may wish to consider but remember this is not an exhaustive list and you should consider the risks that relate to your initiative).

The template in Appendix C includes a risk assessment approach which should be followed and if appropriate the risk should be transferred to the risk registers by the Information Asset Owner and to the project risk log. There is the optional table in Step 4 to measure the risk score.

Does a DPIA need to be completed for every initiative?
You must complete the screening questions for every initiative. However you will only need to complete the full DPIA for initiatives that include personal information and for which a screening question has been answered as yes.

---

8. Monitoring/ review

This policy will be subject to review by the Trustees to include effectiveness, compliance and the quality of the assessments completed.

---

9. Associated documentation

In completing a DPIA you may need to refer to information governance associated policies and guidance.

---

10. Appendices

Appendix A – Potential privacy risks

Appendix B – Overview of the DPIA process

Appendix C – DPIA template – screening questions and assessment

---

Appendix A – Potential privacy risks

Risks to individuals can be categorised in different ways and it is important that all types of risk are considered – these range from risks to physical safety of individuals, material impacts (such as financial loss) or moral (for example, distress caused). Possible risks include:

Risks to individuals

Inadequate disclosure controls increase the likelihood of information being shared inappropriately. The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.

- New surveillance methods may be an unjustified intrusion on their privacy.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- Identifiers might be collected and linked which prevent people from using a service anonymously.
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary.

Corporate risks

- Non-compliance with the UK GDPR or other legislation can lead to sanctions, fines and reputational damage.
- Problems which are only identified after the project has launched are more likely to require expensive fixes.
- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the Trust.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of confidence.
- Data losses which damage individuals could lead to claims for compensation.

Compliance risks

- Non-compliance with the UK GDPR
- Non-compliance with the Privacy and Electronic Communications Regulations (PECR)
- Non-compliance with Trust specific legislation or standards
- Non-compliance with human rights legislation

Appendix B – Overview of the DPIA process

Step 1: Identifying the need for a DPIA
The need for a DPIA can be identified using the screening questions included in the DPIA template – see Appendix C.

Step 2: Describing the information flows
Describe the information flows of the initiative. Explain what information is collected, used, what it is used for, who it is obtained from and disclosed to, who will have access, and any other necessary information. For existing data establish that original consent and privacy notices cover the work being planned/undertaken.

Step 3: Identifying the privacy and related risks

- some will be risks to individuals – for example damage caused by inaccurate data or security breach, or upset caused by unnecessary intrusion on privacy.
- some risks will be to the organisation – for example damage to reputation, or the financial costs of a data breach.
- legal compliance risks include the UK GDPR, PECR, and the Human Rights Act.

Step 4: Identifying and evaluating privacy solutions
Explain how you could address each risk. Some might be eliminated altogether. Other risks might be reduced. Most initiatives will require acceptance of some level of risk, and will have some impact on privacy.

Evaluate the likely costs and benefits of each approach. Consider the available resources, and the need to deliver a project which is still effective.

Step 5: Signing off and recording the DPIA outcomes
Privacy risks must be signed off at an appropriate level as part of the decision making process.

A DPIA report should summarise the process, and the steps taken to reduce the risks to privacy. It should also record the decisions taken to eliminate, mitigate, or accept the identified risks.

Publishing a DPIA report will improve transparency and accountability and lets individuals learn more about how your project affects them.

Step 6: Integrating the DPIA outcomes back into key documentation
The DPIA findings and actions should be integrated back into key documentation – the DPIA template in Appendix C provides a list of documentation to consider. It might be necessary to return to the DPIA at various stages of the initiative's development and implementation. Large initiatives are more likely to benefit from a formal review process.

A DPIA might generate actions which will continue after the assessment has been finished and these must continue to be monitored.

Record what you can learn from the DPIA for future initiatives.

Appendix C – DPIA template for screening questions and completing an assessment

Initiative name
Version and date

The following screening questions will identify if a DPIA is required. Answering ‘yes’ to any question will require a DPIA to be completed. You may expand on the answers as work progresses.

Number	Question	No	Yes	Comments
1	Will the initiative involve the collection of new information about individuals?			
2	Will the initiative compel individuals to provide information about themselves?			
3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? NB. This includes individuals who have previously accessed information but now work for a different organisation.			
4	Will you be 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 initiative involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.			
6	Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?			
7	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.			
8	Will the initiative require you to contact individuals in ways which they may find intrusive i.e. invasive, indiscreet, interfering or upsetting?			

If all questions have been answered ‘no’ a copy of this document should be retained in accordance with our records retention policies and as the initiative develops reference made to the screening questions in case any answers change to ‘yes’. If any question has been answered ‘yes’ please continue to complete the rest of this template.

Step one – Identify the need for a DPIA

Initiative outline Note – explain what the initiative aims to achieve, what the benefits will be to the organisation, to individuals and to other parties. You may find this information in management reports, committee papers, a project mandate, brief or PiD.	
Why is a DPIA required? Note – this can draw on your answers to the screening questions.	

Step two – Describe the information flows

Information flows Note – describe how personal information is collected, stored, used and deleted explaining what information is used and what is it used for and who has access to it. It may also be useful to refer to process diagrams or another way of explaining data flows. To obtain a full understanding of information flows it is important that you consider <u>all</u> of the following information: ● How many individuals will be affected? ● How information is collected? ● Why is information collected? ● How will the information be stored? ● For how long will the information be stored? ● Where has information come from? Who will have access to the information? ● How will information be deleted?	

• Can analysis or reporting of anonymised data sets identify an individual? • Can combining various sets of data result in the identification of an individual? • Potential risks with the information flow? • For use of existing data does the consent form/s used to collect the original data, and the associated privacy notices, cover the use of the data being considered by the initiative.	
Advice sought and consultation Note – explain what practical steps you will take to ensure that you identify and address privacy risks. Who needs to provide advice? Who should be consulted, internally and externally? How will you obtain advice and carry out consultation?	

Step three – identify the privacy related risks

Note – identify the key privacy risks and the associated legislative compliance and corporate risks. Annex 1 provides an extract of the UK GDPR principles to help you identify where there is a risk that the initiative will fail to comply with the UK General Data Protection Regulation or other relevant legislation, for example the Human Rights Act.			
	Consequence		
Privacy risk/ issue	Identify risks to individuals	Identify legislative compliance risks	Identify associated organisation/ corporate risk

Step four – identify privacy solutions

Use either one of these two options to identify privacy solutions depending on the nature of the initiative and the risks involved

Step 4 – Optional – to support risk assessment measurement

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

You will need to score the privacy risk by multiplying the impact of the risk happening (1-3) by the likelihood of the risk happening (1-3) using the key shown in the table below. Once you have identified the solutions (mitigating actions/ opportunities) to manage or mitigate the privacy risk you need to calculate the residual score. Any privacy risk with a residual score of 6 or more should be considered high risk.

	Impact (I)	Likelihood (L)	Score (S)
1	No or slight impact	Unlikely to happen	I x L
2	Significant impact	Possible to happen	
3	Major impact	Highly likely to happen	

Ref	**The Risk** What can happen and how it can happen	**Consequence / benefit of event happening**	**Inherent Risk**			**Mitigating Actions / Opportunities**	**Residual Score**			**Further Action Required**	**Risk Owner**	**Open/ closed**
			I	L	S		I	L	S			

Step 4 – Option 2 – preferred method

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

Note – who has approved the privacy risks and solutions involved in this initiative? Who is responsible for implementing approved solutions?		
Risk	Approved solution	Approved by whom and date

Step six – Integrate the DPIA outcomes back into the key documentation

Note – who is responsible for integrating the DPIA outcomes back into the key documentation? Who is responsible for implementing the solutions that have been approved?			
Action to be taken/DPIA outcomes	Key Documentation	Date for completion of actions	Responsibility for actions

Annex 1 – Linking the DPIA to the UK General Data Protection Principles

This annex will help you identify where there is a risk that the initiative will fail to comply with the UK General Data Protection Regulation or other relevant legislation. The principles listed are those set out in Article 5 of the UK General Data Protection Regulation with italic notes explaining the information you need to consider.

NB - The wording refers to projects using a broad definition and for the purposes of conducting a DPIA should be applied to any initiative.

Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

Have you identified the purpose of the project?

How will individuals be told 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?

Are your actions a proportionate response to the need?

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?

(b) 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

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

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

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

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

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

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

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?

(e) 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; 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

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

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

(**f) 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 ('integrity and confidentiality').**

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?

In addition to the Principles in Article 5, Chapter V covers data being transferred to another country outside the UK

Will the project require you to transfer data outside of the UK?