AQUILA Diocese of Canterbury Academies Trust

Multi Academy Trust Policy

Common Trust Policy, Use as Published

Data Protection Impact Assessment & Procedure Policy

Date adopted by Trust Board: January 2024

Date of next Review: January 2027

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 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. 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 school 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 school 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 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.

PCER

The **Privacy and Electronic Communications (EC Directive) Regulations** 2003 is a law in the United Kingdom enacted to protect data and privacy by making it illegal to send marketing communications without prior permission from the recipients.

2. Background Information

Completion of a Data Protection Impact Assessment (DPIA) is a requirement of Article 35 of the General Data Protection Regulation.
With so much information being collected, used and shared in the school, 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 Trust Board through the local governing body has overall responsibility for the strategic direction and governance of the school, including ensuring that school processes comply with all legal, statutory and good practice guidance requirements.

The Head Teacher is responsible to the governing body 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 school 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 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 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 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 school through better policies and systems being produced and improving relationships with individuals.

6. The DPIA process

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 D.

How do I complete a DPIA?
The template attached at appendix D 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 school 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 a 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 school. It is the responsibility of the school 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, treated, 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 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 school; 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 D 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.

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 Trust to include effectiveness, compliance and the quality of the assessments completed.

9. Appendices

Appendix A – Potential privacy risks
Appendix B – Useful links
Appendix C – Overview of the DPIA process
Appendix D – DPIA template – screening questions and assessment

Appendix A – Potential privacy risks

The Information Commissioner's Office (ICO) 'Conducting privacy impact assessments code of practice 20140225' version 1.0 details possible privacy risks. This appendix details the relevant extract from the code of practice.

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 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 school.

• 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 GDPR

• Non-compliance with the Privacy and Electronic Communications Regulations (PECR)

• Non-compliance with school specific legislation or standards

• Non-compliance with human rights legislation

Appendix B – useful links

Information Commissioner's Office - Conducting privacy impact assessments code of practice 20140225 version 1.0
https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf

Information Commissioner's Office - Anonymisation: managing data protection risk code of practice
https://ico.org.uk/media/1061/anonymisation-code.pdf

Information Commissioner's Office - Data sharing code of practice
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/

Appendix C – 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 D.

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 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 D 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 D – DPIA template for screening questions and completing an assessment

Project Title:	
Brief project summary (please keep this very short. One paragraph should be sufficient)**:**	
Name of Responsible person:	**Position:**
Responsible School/Service:	
Timing of the project (start/end dates, duration, as applicable)	
Date form completed:	

Screening questions
When responding to the questions listed below, please consider each question carefully in relation to all aspects of the project as this screening form and associated DPIA may be used to evidence our compliance with UK GDPR.

1	Will the project involve the collection of new information about individuals?	Yes ☐ No ☐
2	Will the project compel individuals to provide information about themselves (i.e. by not providing the information the individuals would be disadvantaged in some way)?	Yes ☐ No ☐
3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Yes ☐ No ☐
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 for?	Yes ☐ No ☐
5	Is the information about individuals a kind particularly likely to raise privacy concerns or expectations including special categories data? For example, health records, criminal records or other information that people would consider to be particularly private.	Yes ☐ No ☐
6	Will the project require you to contact individuals in a way which they may find intrusive e.g. telephoning or emailing without their prior consent or knowledge?	Yes ☐ No ☐
7	Will the project replace a function that previously required specialist support by introducing new facilities to gather, process, analyse or share personal data?	Yes ☐ No ☐
8	Will the project involve the processing of personal data by third parties (third parties would include all cloud based services) or sharing	Yes ☐ No ☐

	information with third parties such as external collaborators/partners?	
9	Will the project expose personal data to elevated levels of security risks (such as a risk to personal safety or financial risks)?	Yes ☐ No ☐
10	Are stakeholders likely to have privacy concerns about the project?	Yes ☐ No ☐
11	Will the project involve children?	Yes ☐ No ☐
12	Will you be using personal data for marketing purposes, including promotional activities?	Yes ☐ No ☐
13	Will you be transferring any personal data outside the UK/EU/EEA?	Yes ☐ No ☐
14	Will you be processing personal data without informing the data subjects?	Yes ☐ No ☐
15	Does the project involve you using new technology or technology which might be perceived as being privacy intrusive? For example the using of biometrics, facial recognition, monitoring via CCTV, automated decision making or profiling.	Yes ☐ No ☐
16	Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	Yes ☐ No ☐
17	Will you be involved in large scale processing (In considering whether your processing is large scale you should take account of the number of people affected by the processing (either as a number or proportion of the relevant population), the volume and range of data being processed, the duration and permanence of processing and the geographical extent of the processing)	Yes ☐ No ☐
18	Will there be any data matching (putting two or more data sets together from different sources)	Yes ☐ No ☐
19	Will you be tracking individuals online or offline location or behaviour in any way (including the use of cookies)?	Yes ☐ No ☐
20	Will you process any personal data that could result in a risk of physical harm in the event of a security breach?	Yes ☐ No ☐

Next steps
Select the appropriate route:

If you have not ticked yes to any questions	→	You do not need to provide any further information but this screening form should be sent to DPO@aquilatrust.co.uk for their records
If you have ticked 3 or fewer yes boxes (excluding questions 14-20)	→	You need to complete the DPIA Short Form
If you have ticked any yes boxes for questions 14 to 20	→	You need to complete a DPIA Long Form
If you have ticked four or more yes boxes	→	You need to complete a DPIA Long Form

If you are completing the short or full DPIA form this screening form should be submitted to the Trusts' DPO DPO@aquilatrust.co.uk along with your completed DPIA form.