Eleanor Palmer School

Data Protection Policy

Headteacher: Kate Frood
Date last ratified by governing body: 28 November 2018
Review date: November 2020

1. Introduction and Scope

1.1 The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 are the laws governing the processing of personal data in the United Kingdom. They apply to anyone that uses or accesses personal data.

1.2 This policy sets out how Eleanor Palmer Primary School processes personal data and complies with the legislation referred to in section 1.1 and covers all processing of personal data whether in electronic or paper formats.

1.3 Eleanor Palmer Primary School is a Data Controller registered with the Information Commissioner's Office (ICO) Z7166969 and must comply with the regulations in the processing of personal data, including the way in which the data is obtained, stored, used, disclosed and destroyed. The school must be able to demonstrate compliance. Failure to comply exposes the school to civil claims and/or enforcement action from the ICO that may include financial penalties.

1.4 Staff, when processing personal data for school business, are acting on behalf of the Data Controller, and for avoidance of doubt, when this policy refers to actions the school shall take, it also means the staff involved with the processing of relevant personal data.

1.5 This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the school. Any failures to follow this policy may result in disciplinary proceedings.

2. Personal Data

2.1 Personal data only includes information relating to natural persons who can be identified or who are identifiable, directly from the information in question, or who can be indirectly identified from that information in combination with other information (for example: name, address, date of birth, National Insurance number, bank account details etc.).

2.2 Personal data may also include special categories of personal data. This is information about racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or condition, sexual life, biometric data. Separate rules also apply in relation to information relating to criminal convictions.

2.3 Eleanor Palmer Primary School will only collect and process this information for specific purposes where allowed by the law (for example equal opportunities monitoring) or where it has asked and received consent to do so.

2.4 The school is required to adhere to the six Data Protection Principles specified in article 5.1 of the GDPR. The school is also required to maintain records that demonstrate this compliance by article 5.2 of the GDPR. This is achieved by this policy document, maintaining a record of processing activities in an Information Asset Register (IAR), and any further policies that are specific to those processing activities.

2.5 This policy deals with the Data Protection Principles in sections 4 through 9.

3. Data Protection Officer

3.1 The school is required by the legislation to appoint a Data Protection Officer (DPO). The Data Protection Officer is Robert Bullett, HR Adviser for the London Diocesan Board for Schools. He can be contacted at Robert.Bullett@london.anglican.org or 020 7932 1161. The Data Protection Officer is supported by Data Protection Advisors that monitor these contact details and carry out business-as-usual tasks on his behalf.

3.2 The role of the Data Protection Officer helps the school to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

3.3 Should data subjects, e.g. pupils, parents, or staff, have concerns or enquiries regarding Data Protection, they should in the first instance discuss these with the school's leadership. But if this is not possible or not practical in the circumstances, they may contact the DPO directly.

4. Fair, lawful, and transparent.

4.1 The school commits to compliance with the first Data Protection Principle by handling Personal Data fairly:

4.1.1 The school will only process Personal Data in ways which would reasonably be expected of a school and will be honest and transparent about the reasons for any processing. Should there be any processing required which may be unexpected or unusual, school leadership in conjunction with the DPO will take steps to inform the subjects as far as reasonably possible under the circumstances. This may take the form of an extra Privacy Notice. (See Section 4.3 (Privacy Notices))

4.1.2 If there may be any adverse effects on data subjects due to processing the school will give consideration to these and be able to justify any such processing. See section 11 – Data Protection Impact Assessments.

4.2 The school commits to handle personal data lawfully by assessing the lawful basis for all significant processing activity. This will be maintained in the IAR, and where necessary, recording in a DPIA.

4.3 The school is committed to transparency and upholding the right of the data subject to be informed of how their data is being processed. This is normally done through providing a copy of, or a link to, the School's Privacy Notice: https://www.eleanorpalmer.camden.sch.uk/wp-content/uploads/2018/06/Privacy-Notice.pdf. Additional Privacy Information may be communicated with data subjects as required.

4.3.1 This Privacy Notice or additional information will be provided at the time the information is collected. Should the information be obtained from a third party, such as the Local Authority or Department of Education, the school will normally provide this information within 30 calendar days.

5. Purposes of processing

5.1 The school shall process data only for the purposes it was originally collected, or compatible purposes. The purposes will be communicated with the data subject in a Privacy Notice as per section 4.

5.2 Should a need arise to process data in an additional or different way to the purposes originally specified, the school's leadership shall consult the DPO regarding a Data Protection Impact Assessment. The new purposes must be found to be lawful and fair, and then communicated transparently as per section 4.

6. Data Minimisation

6.1 The school will not collect more data than it requires. For significant processing activities, the Information Asset Owners listed in the IAR will be responsible for ensuring that only the minimum information required for the specified purpose is held, and no more. Often this will involve reviewing forms that are used to collect data, and ensure that there are not fields collecting information that is no longer used.

6.2 For any other processing carried out on behalf of the school, the staff carrying out the processing will be responsible for compliance with this principle. In summary, staff should assess the need to collect personal data before doing so, and only collect personal data when necessary, and then only the minimum data required.

7. Data Accuracy

7.1 For significant processing activities, the Information Asset Owners listed in the IAR shall be responsible for ensuring accuracy of data. This will involve an assessment of the risks associated with the data being or becoming inaccurate and implementing an appropriate procedure for ensuring the data obtained is accurate and is kept accurate.

7.2 Individual staff remain responsible for keeping and maintaining their own accurate records for any other processing undertaken.

8. Retention and Destruction

8.1 Personal data shall be kept only for as long as it is required for the purpose it was collected for and no longer.

8.2 The school complies with the IRMS Guidance on Retention of Records ("IRMS Guidance"), which can be found at the following web address: https://www.ldbsact.org/docs/policies/data_protection_policies_/Data_Protection_Policy_-_Data_Retention_Schedule_-_May_2019.pdf to specify how long information is kept for. It also specifies how it is disposed of at the end of this period.

8.3 The Information Asset Owners are responsible for ensuring deletion/destruction is carried out in accordance with the IRMS Guidance, and also for keeping the necessary records to show that data have been appropriately destroyed.

8.4 Other records (those not included in the Asset Register) may also be included in the IRMS Guidance to assist with managing files. Staff will seek advice if uncertain about how long they should be keeping a record.

9. Information Security

9.1 For significant processing activities, the Information Asset Owners listed in the IAR shall be responsible for carrying out a risk assessment and ensuring security measures in place adequately reflect the risks associated with that processing. This is in addition to any basic requirements set out below.

9.2 **Digital Technology**

9.2.1 The school will ensure that all data held on its IT systems is held in accordance with the principles of the Data Protection Act 2018. Data will be held securely and password protected with access given only to staff members on a "need to know" basis.

9.2.2 Pupil data that is being sent to other organisations will be encrypted and sent via a safe and secure system such as School2School or Egress. Any breaches of data security should be reported to the head teacher immediately.

9.3 Alongside our online safety policy, staff:
9.3.1 do not disclose passwords to anyone
9.3.2 do not email sensitive personal information to their own personal email accounts
9.3.3 use secure email facilities such as Egress to send sensitive personal information to external organisations
9.3.4 only use USB memory sticks that are encrypted
9.3.5 have their IT access taken away if they no longer work for the school

9.4 **Paper and other hard copy data**

9.4.1 Staff must store data securely at all times and should never store data, even temporarily, where it may be at risk (e.g. staff must not take data to a pub or restaurant on the way home, or leave it in the back of a car overnight or when at the supermarket).

9.4.2 Paper based information should only be carried outside the organisation if absolutely necessary and only with the explicit approval of a member of the SLT.

9.4.3 This information should not be read or displayed on public transport, or in public spaces due to the risk of unauthorised disclosure.

9.4.4 Where it is absolutely necessary to keep confidential information at home (for example key emergency contact details or business continuity plans) as sanctioned by a manager with the necessary authority, these documents must be kept securely under lock and key. This means that such information should be stored in a private lockable cupboard or similarly secure space, and should be kept out of sight (e.g. not left on tables or in hallways where it would be visibly obvious to unauthorised persons, such as housemates, or intruders).

9.4.5 Paper based information should also be stored separately from high value items such as laptops wherever possible, and should not be kept together in a laptop bag.

9.4.6 Staff must ensure they know who to contact for security advice and guidance, including when working remotely, and how to contact them.

10. Automated processing and decision making

The school does not carry out any automated processing or decision making using personal data.

11. Individual Rights

11.1 **Subject Access**

11.1.1 Individuals ("Data Subjects") have the right to access their personal data. The person who the personal data is about is known as the data subject and the person who is making the

request is known as the applicant. These can of course be the same person depending on the personal data sought. A common example of this relationship would be when a parent (applicant) is seeking personal information about their child (data subject).

11.1.2 To request access to personal data that the school holds about a Data Subject, a Subject Access Request (SAR) form can be completed and submitted to the School. SAR forms may be obtained from the school office. The form is not a requirement as a valid request does not have to be in a specified format. But for convenience of record keeping the school requests that applicants use the form.

11.1.3 Parents may request information about their children. However, the legislation specifies that the rights over personal data rest with the subject of that data, providing that the subject has sufficient maturity and competency to understand their rights. There is no prescribed age specified in the legislation for this, but other parts of the legislation indicate that 13 is a reasonable starting point. This means that in the case of any child (including those under the age of 13) refusing to allow disclosure, an assessment must be made of their competency. If a child is assessed as competent then their control over their personal data for these purposes cannot be overridden by the wishes of the parents.

11.1.4 The school must take sufficient steps to be satisfied of the identity of the applicant and their right to the information. To these ends, the school may request any identification documents reasonably necessary to establish identity. These will normally include:

11.1.4.1 one piece of photographic identification, such as a valid passport, valid driving licence or a valid EU national identity card.

11.1.4.2 one piece of identification confirming address and dated within the last three months such as a utility bill, council tax statement or bank statement.

11.1.5 There is no fee for a Subject Access Request. Where a request is manifestly unreasonable or excessive then the school will opt to refuse the request rather than charge a fee as allowed by the legislation.

11.1.6 The school has one calendar month to respond to a subject access request. This may be extended in some circumstances which will be explained at the time they occur.

11.1.7 The details in this policy are a summary only. The school will manage Subject Access with due regard to the Information Commissioner's Office Subject Access Code of Practice, and where necessary, in consultation with the Data Protection Officer.

11.1.8 A separate right exists under the Education (Pupil Information) (England) Regulations 2005 (SI 2005/1437) for parents to view their child's Educational Record free of charge. However, a charge may be made for providing a copy of these documents.

11.2 **Other individual rights**

11.2.1 Further rights provided by the legislation and relevant to the processing carried out by the school are:

- Right to rectification
- Right to erasure (Right to be forgotten)
- Right to restrict processing
- Right to object to processing

11.2.2 The school will uphold these rights in accordance with the legislation. Individuals wishing to know more about these rights should be referred to the Information Commissioner's Office website. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

11.2.3 To exercise their rights data subjects should contact the School Business Manager.

12. Closed Circuit Television (CCTV)

12.1 The school uses CCTV for the purposes of:

12.1.1 Monitoring entrance to the school and allowing office staff to observe visitors.

12.1.2 Security and crime prevention

12.2 CCTV is recorded.

12.2.1 Recordings are only kept for 90 days unless specifically marked for retention. For example, when it is known that an incident has been recorded and the school decides the footage will be retained.

12.2.2 Footage retained will be kept for as long as necessary to serve the purpose it was retained for and the school will review retained footage annually to determine if it is still required and dispose of any that is not, in line with the IRMS Guidance.

12.3 The school's CCTV manager is the School Business Manager and they are responsible for ensuring CCTV is managed in line with the ICO's CCTV code of conduct.

13. Information Asset Register

13.1 The school is required by Article 30 of the GDPR to keep a record of data processing activities. This is maintained in the IAR.

13.2 For each Asset listed in the IAR, there will be specified:

13.2.1 The purposes the information is used for.

13.2.2 The categories of data subjects (e.g. students, parents, staff)

13.2.3 The categories of personal data (e.g. contact details, educational records, employment records)

13.2.4 The retention period for that data, or link to the IRMS Guidance.

13.2.5 Details of any transfers to international organisations or third party countries.

13.2.6 Security measures protecting the data

13.2.7 The condition(s) under Article 6 and/or Article 9 of the GDPR that allow the processing

13.2.8 The lawful basis relied on for the processing

13.2.9 The details of any joint Data Controllers

13.2.10 The information necessary to demonstrate compliance with any of the other functions referred to in this policy. e.g. sections 4 through 9.

13.2.11 The Information Asset Owner (IAO)

13.3 The maintenance of this register will be overseen by the School Business Manager and the responsibility for ensuring each entry remains accurate and is regularly reviewed lies with the corresponding IAO.

14. Information Sharing with third parties / joint controllers / processors

14.1 The school shall only share data with third parties when the following conditions are met:

14.1.1 There is a contract in place with specifying how the third party will process data on behalf of the school.

14.1.1.1 All contractors are required to meet specified data security standards, and have adequate policies in place.

14.1.2 There is a written Information Sharing Agreement in place with another Data Controller such as the Local Authority or another school which describes the responsibilities of both parties.

14.1.3 An exemption applies which allows or requires the school to disclose data to that third party (for example, to assist with police investigations or by the order of the courts).

14.1.3.1 Police or other parties asking the school to disclose data for these purposes should contact us on admin@eleanorpalmer.camden.sch.uk or by telephoning 020 74852155

14.1.4 Where other conditions set out in regulation 6 and/or regulation 9 of the GDPR apply and permit personal data to be shared. E.g. the subject has given consent.

14.2 The school does not store or transfer data outside of the European Union.

15. Data Breaches

Please refer to separate Data Breach Policy.

16. Privacy by design and default, and Data Protection Impact Assessments (DPIA)

16.1 Whenever the school is implementing a new system or business practice that involves the processing of personal data, the school will observe privacy by design.

16.2 A DPIA is a risk based approach required by the GDPR to identify and manage high risk processing by identifying it and associated risks early.

16.3 All new projects or systems which involve a significant amount of personal data processing require a DPIA screening questionnaire to be completed by the project manager.

16.4 The screening questionnaire shall be submitted to the school's management and the DPO, who will advise on the risks and whether a full DPIA is required.

16.5 For those projects considered to be High Risk, or otherwise requiring a full DPIA, the School Business Manager and the DPO will prepare the full DPIA for submission to the governing body for approval before the project is able to proceed.

16.6 The screening questionnaire, the full DPIA, and associated guidance about how to complete these is found at Appendix 1.

17. Photography

17.1 The school uses photographs of individuals for the following purposes:

17.1.1 Security and access purposes (ID cards or passes)

17.1.2 To assist staff with the identification of pupils with allergies

17.1.3 Class photographs – records for posterity.

17.1.4 Our own publications – such as newsletters, our website, or the prospectus.

17.1.5 Providing photographs for other media to use in their publications.

17.1.6 Photographs of adults participating in our teacher training and NQT programme for identification purposes.

17.2 Consent will be sought for the use of photographs when that child joins the school and no photographs will be taken of children who have not been provided with consent except where the use of photograph is considered essential to the operation of the school or the safety of pupils

18. Telephone Call Recordings

The school does not record telephone calls.

19. Biometrics

19.1 Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.

19.2 The School does not record biometric data.

20. Consent

20.1 In order to process personal data, the school relies primarily on the conditions provided by regulation 6(1)(c) (legal obligation) or 6(1)(e) (public task). The condition provided by 6(1)(a) (consent) will normally only be used when another does not apply.

20.2 When consent is used as the basis for processing, the school shall request consent and that request shall:

20.2.1 Be in writing.

20.2.2 Require a positive action to "opt in" or give consent.

20.2.3 Be clear and concise and where consent is being asked of a child; extra care shall be taken to phrase the consent in terms they are likely to understand.

20.2.4 As far as practicable in the circumstances, be specific and granular to avoid blanket consent or any other possible confusion.

20.2.5 Be provided alongside a Privacy Notice. (See section 4.3 of this policy)

20.3 The school will explain that it will always be possible for consent to be withdrawn at any time after it has been given, although if the processing has already occurred it may not be possible to reverse that. e.g. If a publication is already printed and distributed, and a subject changes their mind about the use of a photograph, the school may only be able to stop the use of that photograph in future publications.

20.4 Processing shall not take place until the consent request has been completed and returned. The consequences of this will be explained in the request.

20.5 Consent from children

20.5.1 The rights provided by the legislation rest with the subject of the data. This means that where the data is about children, and where the child has sufficient maturity and understanding, the child may exercise their right to consent, or withdraw consent, as appropriate. There is no fixed age provided by the legislation, but as a starting point, children aged 13 years or older will be informed of consent requests and their associated rights.

20.6 The school will maintain sufficient records of consent to be able to demonstrate that consent has been given or withdrawn for any processing of personal data relying on consent until that processing has ceased.

21. Review

This policy will be reviewed annually by the School Business Manager. This policy is subject to as required by developments in case law or guidance issued by the ICO or other official body. Changes may occur without advance notice.

Version control

Date:

Updated by:

Appendix 1

The Data Protection Impact Assessment (DPIA) will enable you to systematically and thoroughly analyse how your project or system will affect the privacy of the individuals (i.e. customers) involved.

- The DPIA is a proactive approach to privacy protection;
- The outcome of a DPIA should be a minimisation of privacy risk;
- Conducting a PIA is a legal requirement under the General Data Protection Regulation (GDPR) if the processing is likely to result in a high risk to the rights and freedoms of natural persons, particularly if the proposed processing is using new technologies. Where the processing is not a high risk and a DPIA is not obligatory, it can be recommended as the most effective way to demonstrate to the Information Commissioner's Office (ICO) how personal data processing complies with the GDPR.

- The purpose of this pre-screening questionnaire is to identify whether the intended processing is high-risk and to record the decision as to whether or not to proceed with a full DPIA.

- If you have an existing project and the risk has changed, carry out this pre-screening questionnaire to find out if a full-DPIA is required, to make sure that your project complies with the GDPR.

Further guidance on completing the Pre-Assessment and Full DPIA is available from the accompanying guidance. Further information on the DPIA is also available on the ICO's PIA code of practice. You should also refer to the Article 29 Data Protection Working Party Guidance to help assess the risk of the proposed processing: http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

GOVERNANCE ARRANGEMENTS

A copy of the completed Pre-Assessment (including the signed declaration where appropriate) must be sent to the Clerk to the CIGG (jim.read@camden.gov.uk) . The Data Protection Officer (DPO) and CIGG will review pre-assessments on a risk basis and at any time during the life of the project, may ask you to attend a meeting to provide further information, answer questions and respond to any privacy concerns.

The DPIA or pre-screening questionnaire may also be requested by the DPO, ICT Project Review Board and ICO at any time.

A decision may also be taken to publish the DPIA, redacted where necessary to preserve appropriate commercial confidentialities. You should not allow the possible publication to affect your completion of the DPIA as any truly sensitive material would be redacted before any publication.

You must keep the signed DPIA and all supporting documents with your project file for audit purposes.

Section One –

Pre-Assessment Completed By		**Date of Completion**	

Project Summary

Project Name		**Directorate and Service**	
Project Sponsor and Position		**Project Manager and Position**	
Project Start Date		**Project Go Live Date (anticipated/planned)**	

Brief Description Of The Project

Purpose of the processing:

Data Categories:

For example, children, vulnerable adults. Residents, users of a service.

Does this project involve data which is already being processed but there is a change in risk? If so, explain the processing that is currently being carried out, explain the change in risk and attach the previous DPIA (if there was one):

Data Processing Summary

1 **Identify the personal data you will be processing and specify the purposes for requesting it** (Please add more lines if necessary)

What is personal data?

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; (GDPR Article 4)

Personal data	What is the purpose?

2 **How will the information be collated and who will have access to it?**

Response:

3 **Will it be transmitted to third parties and how?**

Response:

4 **How will it be stored, kept up to date and disposed of when no longer required?**

Response:

5 **What stakeholders are involved or will be affected by the project?**

Response:

6 **Are there any previous projects of a similar nature? If so what good practice could be taken from these with respect to data privacy protections?**

Response:

Section Two - Screening Questionnaire

This section will help you to decide whether a full DPIA is required. Answering **YES** to any of the questions 1-8 is an indication that a full DPIA may be required.

1. **Will the project involve the collection of personal (personally identifiable) data about individuals, either from existing systems and/or directly?**

Yes / No

2. **Will the project compel individuals to provide personal data about themselves?**

Yes / No

3. **Will the project involve the gathering and/or consolidation of personal data from multiple sources?**

Yes / No

4. **Where multiple sources will be accessed, will the personal data be used in a new way, e.g. for a different purpose to which it was originally gathered and consented to?**

Yes / No

5. **Will the personal data be disclosed to other parties, both internal and external, who have not previously had routine access?**

Yes / No

6. **Will the project result in you making decisions to taking action against individuals in ways that can have a significant impact on them?**

Yes / No

7. **Will the project require you to contact individuals in ways that they may find intrusive?** Yes / No

8. **Will the project involve any of the following?**

"(a) a systematic and extensive evaluation of characteristics about individuals based on automated processing, including profiling.

Yes / No

If so, will any decisions based on that automated processing have legal or significant effects on individuals?

Yes / No

(b) processing on a large scale of special category data or personal data relating to criminal

convictions and offences? Special category data is information about a person's race or ethnicity, sex life or sexual orientation, health (including mental health), religious or philosophical beliefs, political views, Trade Union status, and genetic and biometric (eg fingerprints) information

Yes / No

or

- (c) a systematic monitoring of a publicly accessible area on a large scale eg CCTV

Yes / No

If you have answered YES to any of the questions above then you may need to undertake a full DPIA. To assess if a full DPIA is needed you need to assess the risk (see question 9). If there is a high risk then you MUST carry out a full DPIA. If the risk is not high you are not obliged to carry out a full DPIA but you might wish to do to as good practice.

9. **Risk Assessment.**

In assessing risk you need to take into account the nature, scope, context and purposes of the processing and carry out an assessment of the impact of the proposed processing on the protection of personal data.

You can get more information on assessing risk in the Article 29 Data Protection Working Party Guidance to assist in assessing the risk: http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

Will the intended processing concern any of the criteria listed below? Answer Yes/No for each criteria. Where yes please give brief details.

a) **Evaluation or scoring** (for example, building behavioural profiles based on usage or navigation on a website) YES/ NO

b) **Automated-decision making with legal or similar significant effect** (for example processing which may lead to the exclusion or discrimination of individuals) YES/ NO

c) **Systematic monitoring** (processing used to observe, monitor or control data subjects eg CCTV) YES/ NO

d) **Sensitive data or data of a highly personal nature** (this include special categories of data). Special category data is information about a person's race or ethnicity, sex life or sexual orientation, health (including mental health), religion, political views, Trade Union status, and genetic and biometric (eg fingerprints) information

e) **Data processed on a large scale** (considering the number of data subjects, volume of data, range of data, the duration or permanence of the processing, the geographical extent)

f) **Matching or combining datasets** (for example from two or more data processing operations performed for different purposes and/ or by different controllers)

g) **Data concerning vulnerable subjects** (such as children, employees, vulnerable adults; any case where there is an imbalance in the relationship)

h) **Innovative use or applying new technological or organisational solutions** (for example, combining finger print and facial recognition for improved physical access control)

i) **When the processing itself prevents data subjects from exercising a right or using a service or contract** (for example, where a bank screens its customers against a credit reference database in order to decide whether or not to offer them a loan.)

State here the level of risk and give reasons:

High risk:

Medium risk:

Low risk:

Section Four - Conclusion and Declaration

It is the responsibility of the Project Manager and Sponsor to assess the risk that the intended processing may pose.

If you have answered **YES** to any of the questions 1-8 in Section 2 then this is an indication that a full Privacy Impact Assessment **may** be necessary.

If the level of risk is deemed to be high in Section 2 question 9 then a full DPIA **must** be carried out. You must now undertake the full DPIA (link to page). Please send a copy of this screening questionnaire to the Clerk to the CIGG (jim.read@camden.gov.uk)

If you have answered Yes to any questions 1-8 but you deem the level of risk in section 2 question 9 not to be high-risk, you must justify this and document the reasons for not carrying out a full DPIA. Send a copy of this screening questionnaire to the Clerk to the CIGG (jim.read@camden.gov.uk) so the DPO can assess and give views. If on review the DPO considers a full DPIA is required you will be informed.

Record the advice of the DPO below:

1 **Based on your responses to the pre-assessment, will a full DPIA be completed?**

Yes / No

2 **If you answered NO please explain and record the advice of the DPO.**

Advice of the DPO:

PRIVACY IMPACT ASSESSMENT <u>NOT</u> REQUIRED I declare that following pre-assessment and to the best of my knowledge, a DPIA **IS NOT** required for this project and for the protection of data/information associated with it in accordance with the GDPR and the Data Protection Act.		
Project Manager Signature and date		Alternately email approval can be attached
Project Sponsor Signature and Date		