Data Protection Impact Assessment (DPIA)

Project Name:	Annual report of the Virtual School to Corporate parenting Panel
Project Manager or Sponsor (PM):	Sarah Bailey
Name of person completing the DPIA if different to (PM):	
Service Team and Department:	Headtecaher Virtual School
Relevant Director and Executive Director:	Shelley Davies Director of Education
Service Area Cost Code:	C10906 C101908 C10910
Information Management Champion(s) for service area:	Lisa Davis
Date DPIA received by the IMT:	
Date approved by DPO:	
Date approved by IMT :	

1 Project Scope

Include the projects aims, potential impact, all individuals involved in the project and those that may be affected by it. The stakeholders should be as broad as possible so that the list can be edited down after consultation)

Completion of annual report on all activities of Virtual School. Summary document containing high level data and some individual examples (Anonymised) from records of Children Looked after

2 Data Description

Answer the questions below so that there is a clear understanding about how the information will be used, who will use it etc. Remember that it's personal information (i.e. information about individuals) that you need to be concerned with. If you do not have answers to all the questions at this time, simply record what you do know.

Whose information is being used? - *Are there additional concerns that need to be considered due to individuals sensitive/ complex circumstances? i.e. vulnerable person*	The whole cohort referrd to, Looked after children, are vulnerable. However, no personal data is used unless anonymised and not identifiable.
What information is being used? - *Consider the nature of this information E.g. Child's social care file*	High level statistics on data for cohort composition and academic results.
Does it include special category or criminal offence date?	no
Can an individual be identified easily from the information?	no
What is the potential impact on privacy of this information? - *What are the risks/ impact to an individual if this information was lost, stolen or manipulated?* - *E.g. could it be sold?*	The data in the report will be in the public domain. It must not be identifiable externally.
Will this change the manner in which we handle, use or protect this information? *e.g. should it be encrypted?*	

3 Consultation process

Consider how to consult with relevant stakeholders.

When did you consult individuals?	
How did you consult individuals?	
If not explain why it is not appropriate.	
Who else within the organisation have you consulted with?	
Do you need to speak with your processor to assist?	
Do you plan to consult information security experts or any other experts?	

4 Assessment of necessity and proportionality of data usage

What is your lawful basis for processing?	
Is consent being relied upon to share the information? Has explicit consent been obtained? Are data subjects able to opt out from giving consent?	
Does the processing actually achieve your purpose?	
How will the information be collected? Verbally, forms, intranet, interview, 3rd party, anonymous)	
Is there another way to achieve the same outcome?	
How will the information be used? *e.g. to write a report*	
Do the individuals know and understand how their information will be used? If there are changes to their information does the privacy notice need to be amended?	
How will it be stored, kept up to date and disposed of when no longer required? *e.g. stored in locked cabinet/securely shredded*	
How will you ensure data quality and data minimisation?	
Who will have access to the information within LBC? - *Include approximate number of users*	
Are there new or significant changes to the way we manage, use, handle or collect this information? - *Include any identified concerns for the individuals, would these changes heighten risks involved*	
Will individuals within an existing database be subject to new or changed handling? - *If yes amendments need to be made to the privacy notice and these individuals need to be informed.*	
What are the internal arrangements for processing this information? *e.g. number of staff who will have access*	
How will the information be updated? *e.g. monthly check*	
Does the project involve the exchange of information outside of the UK and are there set standards for how the information will be treated? How will you safeguard international transfers?	
How will you prevent function creep?	

5 Assessment of the risks to the rights and freedoms of data subjects

You must describe the source of risk and the nature of potential impact upon individuals and identify any additional measures to mitigate those risks.

5a Security

Who will be responsible for the control for this information?	The report will be publicly available
How will the access to this information be controlled?	
Is the data correctly managed to reduce the risk of collateral intrusion to the data subject?	
Are there adequate provisions in place to protect the information? If so what are they? *e.g. Process, security*	

5b Sharing

Who is the information shared with, why are we sharing the information with this organisation?	The information is to justify use of public funds on services for Children in care and care leavers
What purpose does the information we are sharing have to the third party? - *Ensure that we only share relevant information and not excessively*	
Who will have access to the information, externally? - *Include approximate number of users* - *Describe any sharing arrangements and what the level of access is. It may help to produce a diagram to show the data flows.*	Anyone it will be avaiable on the web
How will it be transmitted to third parties and when? How often?	
Is there a data sharing agreement in place?	
At what stage will the information be transferred?	

5c Identified Risks and assessment:

You should take into account the sensitivity of the information and potential harm that inappropriate disclosure or use of the information could cause to any individuals concerned. You should also consider the reputational loss to the Council and the potential for financial penalties being imposed by the ICO.

To assess the level of risk you must consider both the **likelihood** and the **severity** of any impact on individuals. A high risk could result from either a high probability of some harm or a lower possibility of serious harm.

The severity impact level and likelihood should be scored on a scale of 1 to 10 with 1 being low severity and 10 high. The two scores should be **added** together. The RAG status is derived from the following scale:

Score:

- 15 to 20 = Red (High)
- 8 to 14 = Amber (Medium)
- Below 8 = Green (Low)

To be completed by Project Sponsor

Risk Identified	Severity of Impact	Likelihood of harm	Overall RAG rating
To focus on info that is shared before consent – is dob/ anon details of the family/ sw/mgr/lawyer/ reasons for eligibility			

6 Identify measures put in place to reduce risk.

You must now identify additional measures you could take to reduce or eliminate any risk identified as medium or high risk in step 5.

To be completed by the Project Sponsor

Risk Identified	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
		Eliminated / reduced / accepted	Low / medium / high	Yes / No

Sign off and Record sheet

Item	Name/date	Notes
Measures approved by: Residual risks approved by:		Integrate actions back into project plan, with date and responsibility for completion. **If accepting any residual high risk must consult ICO before going ahead**.
DPO advice provided:		**Summary of DPO advice:** *(DPO should advise on compliance, measures to mitigate risk and whether processing should proceed)*
Consultation responses reviewed by:		If your decision departs from individuals views you must explain your reasons.
DPIA to be keep under review by:		

If you require further guidance to complete this DPIA please contact:

Information Management Team (IMT)
Ext: 47777
Email: information.management@croydon.gov.uk

Data Protection Officer
Email: DPO@croydon.gov.uk