Public

DERBYSHIRE
County Council

Information Security Document

Domestic Abuse Notifications: Early Reporting onto Schools Privacy Impact Assessment

Version 0.2

Version History			
Version	**Date**	**Detail**	**Author**
0.1	30/04/2018	PIA-CMS	
0.2	20/06/2018	Updated Risk	
0.3			
0.3			
0.4			

CONTENTS

Contents	Page
Section 1 - Privacy Impact Assessment Screening Questions	4
Section 2 - Privacy Impact Assessment:	
- Step one: Identify the need for a PIA	5
- Step two: Describe the information flows	7
- Consultation requirements	8
- Step three: Identify the privacy and related risk	9
- Step four: Identify privacy solutions	11
- Step five: Sign off and record the PIA outcomes	13
- Step six: Integrate the PIA outcomes back into the project plan	13
Section 3 - Linking the PIA to the Data Protection Principles	14

Section 1 - Privacy Impact Assessment Screening Questions

Will the project involve the collection of new information about individuals?	NO
Will the project compel individuals to provide information about themselves?	NO
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	YES
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	NO
Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	NO
Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	NO
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 private.	YES
Will the project require you to contact individuals in ways that they may find intrusive?	NO

Section 2 - Privacy Impact Assessment

Step one: Identify the need for a PIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.
You may find it helpful to link to other relevant documents related to the project, for example a project proposal.
Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

Stopping Domestic Abuse Together is a partnership approach for notifying Schools of Domestic Abuse incidents which Derbyshire Police attend where Children are present or those involved have children, or children ordinarily live at the address. The purpose of these emails is solely for the purpose of Stopping Domestic Abuse Together. (The Legal Basis for disclosure: – Sections 10 and 11 of the Children Act 2004 provides the power for the Police and Local Authorities to make arrangements to improve the well-being of children, including their emotional well-being.)

Notifications will be sent via an automatic process when Police Officers complete the DASH through PRONTO and add details of child/children and select a school from the drop down list. An automated email will be securely sent to Derbyshire County Council stating the Name of the Child, the DOB of the Child, whether the child was present or not at the incident and that an incident took place at a specified date and time. A link will be provided on the email directing schools to Derbyshire County Council safeguarding processes and documentation on the Stopping Domestic Abuse Together process. All emails sent through this process are classified - Official Sensitive. The emails should not be shared beyond this agreement and should be stored securely.

Step two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Derbyshire County Council will move the emails once a day onto the Perspective Lite system. The email disclosure is intended only for onward secure transmission to the relevant “Key Adult” by secure email to the specified school.

Derbyshire Constabulary take responsibility for ensuring the naming convention on all emails is correct and as such the onward secure transmission is to the relevant school.

Derbyshire County Council will retain a copy of the email notification up to the point the email is sent to schools via the Perspective Lite System. Following this, the email will be deleted from the Council’s designated secure email account.

The notification to schools will remain on the Perspective Lite system and supporting secure file shares for up to 4 months, after which it will be deleted.

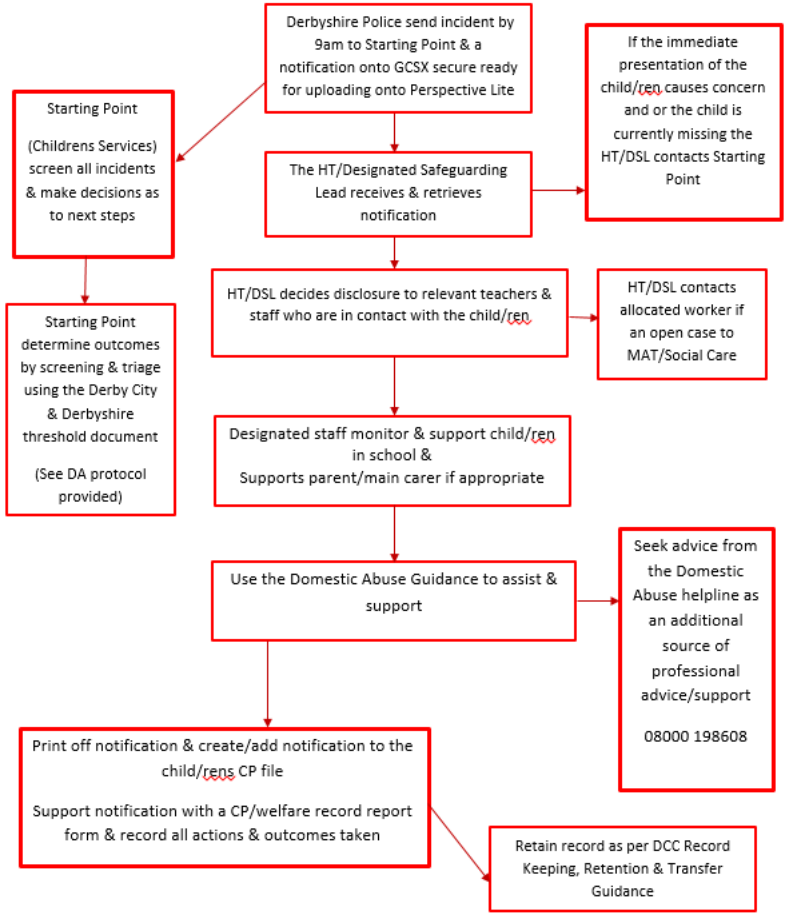
Within Children’s Services the CAYA Web team will be solely responsible for this task as part of their daily tasks.

Derbyshire Constabulary process –

Version 1 April 2018

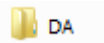
DERBYSHIRE County Council

Domestic Abuse Notifications: Early Reporting onto Schools

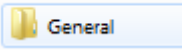


DCC process – Secure area – Receipt and management of Domestic Abuse (DA) files:

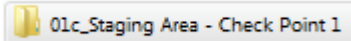
From May 2018, Domestic abuse files will be sent to us from the police via GCSX. We should download to process via Perspective Lite. An initial check for files and upload should be done first thing, with another check later that morning
These DA files are NOT to be opened/ viewed by the web team.
If a DA file is incorrectly named, it must be returned straight back to the sender via GCSX with an explanation of why it has been rejected. The web team are not to rename or alter DA file names in any way.

If correct, the DA files will be placed in the **To Schools_DA** folder 

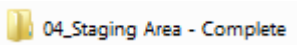
prior to the validation script being run.

Once the script has successfully run, the DA files will be automatically be transferred to the GENERAL 

folder in

01c_Staging Area – Check Point 1 

for processing and uploading to schools in the normal way.
Once successfully uploaded, all DA files must be immediately DELETED from the compressed zipped folder prior to it being saved in **04_Staging Area – Complete** folder.

Save the remaining files in the zipped folder in the normal way to the 04_Staging Area – Complete folder 

Files uploaded to schools will remain on Perspective Lite for upto 4 months until deleted during the routine monthly process.

The police have been sent a file with all schools and DfE numbers. However, when a school becomes a sponsored academy it changes its DfE no, so once this has been amended within Perspective a notice advising the police should be sent to:

Claire Hammond Claire.Hammond.14674@Derbyshire.PNN.Police.UK

Pauline Allgood Pauline.Allgood.5308@Derbyshire.PNN.Police.UK

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the PIA process.

Derbyshire Constabulary and Derbyshire County Council have been working together to develop a protocol, data sharing agreement and process flowchart to address this initiative. Wider consultation has not been appropriate due to the sensitive nature of the information. Schools/Head teachers have attended sessions to discuss the new arrangements and responsibilities. Communications will be placed on SchoolsNet detailing the flowchart and processes.

Derbyshire County Council have asked that schools have added the Stopping Domestic Abuse Together process to advise parents of the disclosure arrangements. DCC have updated the Domestic Abuse Guidance.

Step three: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.
Section 3 can be used to help you identify the DPA related compliance risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk
System data is accessed by unauthorised persons and used or shared inappropriately.	Risks to the individual as a result of contravention of their rights in relation to privacy, or loss, damage, misuse or abuse of their personal information	Breach of Principle 7 of the Data Protection Act	Financial and reputational damage. Legal action could be taken against the LA and possible substantial fine
Retention schedule is not adhered to.	Data is kept for longer than agreed.	Breach of Data Protection Principles 4 and 5	Financial and reputational damage
Notification sent to incorrect school	School is notified of an incident not relating to one of their pupils	Breach of Data Protection Principle 4	Reputational damage as seen as a DCC inaccuracy.

Step four: Identify privacy solutions

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

Risk	**Solution(s)**	**Result:** 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?
System data is accessed by unauthorised persons and used or shared inappropriately.	Access to the system will be limited to only those with the correct role based access activity. The use of the system will be managed locally through relevant training and guidance. Documented Data Sharing Agreement in place.	Accepted/Reduced	
Retentions schedule is not adhered to.	A dedicated retention process has been developed. Any data that has met the retention expiry date will be deleted. Documented Data Sharing Agreement in place.	Eliminated	
Notification sent to incorrect school	Ensure Police have correct DfE numbers. Remove any incorrect DfE numbers and	Reduced	

	incorrectly named files before uploading to Perspective Lite.		

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by
As outlines in step 4	As outlines in step 4	

Step six: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action
Inform key stakeholders of PIA outcomes	8th May 2018	
Update CS retention schedule	8th May 2018	
Update CS Privacy Notice	8th May 2018	
Update CS Information Audit	8th May 2018	
Contact point for future privacy concerns		

Section 3 - Linking the PIA to the Data Protection Principles

Answering these questions during the PIA process will help you to identify where there is a risk that the project will fail to comply with the DPA or other relevant legislation, for example the Human Rights Act.

Principle 1 - Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless: **a) at least one of the conditions in Schedule 2 is met, and** **b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.**	
Have you identified the purpose of the project?	Yes
How will you tell individuals about the use of their personal data?	Privacy Notices
Do you need to amend your privacy notices?	Yes
Have you established which conditions for processing apply?	Yes
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?	N/A
If your organisation is subject to the Human Rights Act, you also need to consider:	
Will your actions interfere with the right to privacy under Article 8?	No
Have you identified the social need and aims of the project?	Yes
Are your actions a proportionate response to the social need?	Yes

Principle 2 - Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.	
Does your project plan cover all of the purposes for processing personal data?	N/A
Have you identified potential new purposes as the scope of the project expands?	No

Principle 3 - Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.	
Is the quality of the information good enough for the purposes it is used?	Yes
Which personal data could you not use, without compromising the needs of the project?	All personal data must be used during this initiative.

Principle 4 - Personal data shall be accurate and, where necessary, kept up to date.	
If you are procuring new software does it allow you to amend data when necessary?	No
How are you ensuring that personal data obtained from individuals or other organisations is accurate?	We are not managing the quality of the information as this is the responsibility of Derbyshire Constabulary.

Principle 5 - Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.	
What retention periods are suitable for the personal data you will be processing?	Dedicated retention schedule put in place.
Are you procuring software that will allow you to delete information in line with your retention periods?	No

Principle 6 - Personal data shall be processed in accordance with the rights of data subjects under this Act.	
Will the systems you are putting in place allow you to respond to subject access requests more easily?	No
If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?	N/A

Principle 7 - Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.	
Do any new systems provide protection against the security risks you have identified?	Yes (Secure File Transfer)
What training and instructions are necessary to ensure that staff know how to operate a new system securely?	New process has been developed and communicated and internal training undertaken, flowchart for all Schools made available via SchoolsNet.

Principle 8 - Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.	
Will the project require you to transfer data outside of the EEA?	No
If you will be making transfers, how will you ensure that the data is adequately protected?	N/A