Restorative Justice & Mediation Services DPIA

Police Fire and Crime Commissioner's Office – Essex

This Data Protection Impact Assessment (DPIA) follows the process set out in the Information Commissioner's Office (ICO) DPIA guidance and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs. For further information please visit: https://ico.org.uk/

Submitting controller details:	
Name of controller	Emma Goddard Restorative Justice Manager
Subject	Restorative Justice and Mediation Services process
Name of DPO	Suzanne Humphreys

Step 1: Identify the need for a DPIA

Delivery of Restorative Justice and Mediation Services.

The Code of Practice for Victims of Crime, section 3, outlines victim's rights to be given information regarding restorative justice. It states:

3.4 If the offender is an adult, you have the Right to receive information about Restorative Justice from the police and how to access Restorative Justice services in your local area. If the offender is under the age of 18, you have the Right to receive information about Restorative Justice from the Youth Offending Team.
4.5 If you report a crime to the police, you have the Right to be referred to a service that supports victims, including Restorative Justice services.

The Police Fire and Crime Commissioner (PFCC) allocates a proportion of the Victim's Grant each year to delivery of an in-house Essex Restorative and Mediation Service (ERMS). In order to provide Restorative Justice, the service receives referrals from a variety of sources including Essex Police, Essex Probation Service, the National Probation Service, local authorities and self-referrals. Referrals are usually made with the service users consent via email to a secure email address or using a contact form on the ERMS dedicated website.

The service is mostly delivered by a team of volunteers, who all consent and provide information in order to support their volunteer role.

A DPIA is required to ensure that risks are addressed around referral pathways and processing of participant and volunteer data.

Step 2: Describe the processing

(a) Describe the nature of the processing:

Referrals are made via an email to a restricted access, secure mailbox (restorativejustice@essex.police.uk.) This email may include an attached referral form.

The contact forms on the dedicated ERMS website, www.restorativeessex.co.uk are also directed to this inbox.

For the majority of cases, initial contact will only be made to participants by ERMS once consent has been sought and secured by the referring agency.
In those instances where a referral is made in which the referring agency is unable to gain consent from all parties, ERMS will seek to find a professional agency working with the participant in order for them to make the initial Restorative Justice offer. On occasions in which there is no professional allocated, or one cannot be found, ERMS will contact the participant directly under the Public Task lawful basis for processing data to inform them of their rights under the Victims' Code and establish if they are interested in knowing more about restorative justice.

Following initial contact from ERMS, in which participants give verbal consent for their data to be stored, participants are provided with a 'consent and confidentiality' form which they are required to sign. Further information may be sought from the referrer before or during ERMS facilitation of a case.

ERMS staff have access to the policing systems - ATHENA and PNC and can therefore look up contact and risk information and case details and police action in order to provide a safe and appropriate service. This access allows the service to quickly access information to prevent delays and revictimisation. These systems are only accessed by vetted, trained, and employed staff using police issued technology.

Once a referral has been accepted, the details of the case from the referral forms/email and ATHENA and PNC data are added manually to ERMS' online case management system, MyRJ. Emails are stored in a dedicated email folder on outlook within the restricted access mailbox and documents are stored electronically in a restricted access folder on the shared drive. When the case has been completed, all emails are transferred to the restricted access folder and deleted from outlook. The electronic files and MyRJ case logs are deleted in accordance with retention policies.

As MyRJ is a cloud-based system, volunteers are able to safely access, manage and update case files from home. Volunteers receive regular training on data protection including how to store and move information securely. All work undertaken on all cases will be recorded on MyRJ. Any paperwork will be scanned/photographed and uploaded or written up into the case notes and then securely stored until it is safely destroyed. The ERMS employed staff have access to all cases stored on MyRJ for oversight and supervision purposes, and volunteer facilitators have access only to their own allocated cases.

Victim and offender information is kept on separate case files and information from one party is only shared with the other with explicit consent. Data will only be shared with the referring agency or other support organisations (unless in safeguarding situations) with consent from the participants. ERMS volunteers currently liaise with other organisations only using initials of the participant as they are often sending from an unsecure email, however, ERMS has set up Criminal Justice Secure Mail (CJSM) secure email accounts for all volunteers, and allocated police issued laptops for those who manage the most serious cases.

Volunteer information is gained with consent and a privacy notice is issued to all volunteers. Personal data is stored electronically in individual files on a restricted-access folder. Any paperwork completed by volunteers is scanned and saved in these folders, and then deleted immediately. Volunteer details are also included in databases in order to provide training and supervision.

See ERMS Retention policy for more information on the data ERMS holds and how long for.

Performance analysis reports are sent out to partners monthly, although this data is anonymised.

(b) Describe the scope of the processing:

Data stored on both volunteers and case participants includes personal data such as their name, address, and other contact details. In addition to this information, special category information such as race, sexual orientation and health data may be stored, if relevant.

ERMS asks volunteer applicants for their monitoring information. The information provided on this form is manually entered onto a database, referring to the volunteer by initials only and the form is destroyed immediately. This information is stored for diversity and equality purposes. We may also have information relating to criminal offences or other special or personal data stored in documents such as supervision records should the volunteer have disclosed this information and consented to it being recorded.

Information relating to case participants (anyone referred to ERMS where the referral has been accepted) will include:

- Police or other agency reference number, and ERMS reference number
- Outcome (e.g. post sentence, community resolution)
- Offence, including a summary and date
- Victims personal information
- Offender personal information
- Personal information of supporters or professionals involved in the case
- Case notes relating to progress and discussions had over the life of the case

Case information will be retained for six (6) years and then destroyed in accordance with the ERMS Retention policy. Rejected referrals are destroyed immediately.

Data will only be stored where it is to our knowledge relevant, accurate, up to date.

Volunteers are recruited from all over Essex and the surrounding areas. Case participants are likely to live in Essex or the surrounding areas, however, may reside anywhere in the country and in a very small number of cases, internationally.

(c) Describe the context of the processing:

ERMS will only use information that is provided with consent sought either directly by ERMS or by the referring agency, which is then confirmed by ERMS. Participants who have not consented to initial contact have their data processed under Public Task in order to gain consent at the first available opportunity.

ERMS will fully explain the restorative justice process and provide a Consent and Confidentiality form which the participants should sign. The form signposts to the PFCC Privacy Notice and outlines the information we hold and what we do with it.

Participants may be adults or children. Anyone who acts as a supporter or appropriate adult also provides consent and their details stored.

ERMS staff are members of the Restorative Justice Council.

(d) Describe the purposes of the processing:

To enable the delivery of restorative and mediation services in Essex. Data is received and processed in order to allow ERMS to provide these services.
The PFCC is obliged to provide information and access to local restorative justice services in line with the Victims' Code of Practice. In discharging these duties through the ERMS it is anticipated that we will improve satisfaction rates of victims of crime and reduce rates of offending or reoffending.

Restorative approaches have been proven to result in high victim satisfaction (94% in Essex) and reduce reoffending rates (14-27% reduction nationally).

Processing data allows ERMS to contact participants to explain the availability of restorative justice. The data gained from the police systems allows us to deliver the service whilst effectively risk assessing and keeping our participants and our volunteers safe.

Step 3: Consultation process

A number of agencies are involved in a referral process, as restorative justice can be offered at any time during and after the criminal justice process.

ERMS holds an Information Sharing Agreement with partners to ensure that referrers are confident and clear on the data security practices of the service and what is expected of them.

The agencies included in the information sharing agreement include:

- Essex Restorative and Mediation Service (Office of the PFCC)
- Essex Police
- Essex District, Borough and City Councils, and Unitary Authorities:
  - Basildon
  - Braintree
  - Brentwood
  - Castle Point
  - Chelmsford
  - Colchester
  - Epping Forest
  - Harlow
  - Maldon
  - Rochford
  - Southend
  - Tendring
  - Thurrock
  - Uttlesford
- Essex County Fire and Rescue Service
- Her Majesty's Prison and Probation Service
- Essex Community Rehabilitation Company
- Essex, Southend and Thurrock Youth Offending Services
- Victim Support
- Restorative Justice services outside of Essex who have signed this agreement

In the completion of this document and data security review, the PFCC office has consulted with Essex Police's Data Protection Officer.

Step 4: Assess necessity and proportionality

As outlined in Section 1 of this document, victims have a right to information and referral to a restorative justice service. The GDPR lawful bases for processing this data are:

- Consent
- Public Task

The processing of this data achieves the purpose of ERMS as it allows agencies to transfer and process data to enable victims and offenders to receive a restorative justice service in line with the code of practice for victims of crime. There is no alternative to gaining the same outcome as without the information provided and processed, ERMS could not contact participants and progress restorative justice outcomes. There is no likelihood of function creep as ERMS delivers a specific service under the guidance of the Victim's Code and the Restorative Justice Council.

The Information Sharing Agreement between partners is regularly reviewed, staff and volunteers are regularly trained on data protection and participants are made aware of how their data will be processed.

Step 5: Identify and assess risks			
Describe source of risk and nature of potential impact on individuals.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Data written down at a face to face participant meeting gets lost	Possible	Significant	Medium
Personal or sensitive information sent to an unsecured email	Possible	Significant	Medium
Case study on website which identifies participants	Remote	Significant	Low
An apology letter is posted on social media	Possible	Severe	High
Release sensitive information to the wrong person	Possible	Significant	Medium
Meetings are video or audio recorded without knowledge or consent of one or more parties	Possible	Significant	Medium
Information passed to another organisation without consent.	Remote	Significant	Medium
Participant refuses to sign form	Possible	Significant	Medium
Illegitimate access to police information	Remote	Severe	Low

Step 6: Identify and assess risks				
Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk** Eliminated Reduced Accepted	**Residual risk** Low Medium High	**Approved** Yes/No
Data written down at a face to face participant meeting gets lost	Volunteers and staff receive annual data protection training to ensure they are aware of how to safely store, transport and dispose of written notes	Reduced	Low	Yes

Personal/sensitive information sent to an unsecured email	Volunteers and staff receive annual data protection training. Part of the facilitator training is to ensure that if they are sending information to a non-secure email that only participant initials are used to prevent identification.	Reduced	Medium	Yes
Case study on website which identifies participants	CJSM accounts are being created for each volunteer to send secure emails and those dealing with the most serious and complex cases are allocated laptops to store, transfer data securely	Reduced	Medium	Yes
An apology letter is posted on social media	Participants sign a form to agree for their story to be anonymously written up as a case study. If they are to be identified, their permission is sought in writing before anything is published. The ERMS Confidentiality and Consent Form includes a clause that participants must not share or publish the outcome of restorative processes. Where an offender writes a letter of apology, the letter is read to the victim but they are not given a copy of the letter to reduce the likelihood of it being used inappropriately. If appropriate to consider the victim keeping the letter, a risk assessment must be completed by facilitators prior to sharing the letter which includes confirmation that the letter writer agrees. Risk assessments are logged on police systems and within MyRJ case system.	Reduced	Medium	Yes

Release sensitive information to the wrong person	MyRJ disaggregates between victim and offender data to prevent accessing information about victims and offenders in the same case. Staff and volunteers are instructed to confirm who they are talking to before divulging any information relating to a case or participants.	Reduced	Medium	Yes
Meetings are video or audio recorded without consent of one or more parties	ERMS's Consent and Confidentiality form clearly states participants do not have permission to record. Facilitators are encouraged to reiterate this at the beginning of each video call.	Reduced	Medium	Yes
Information passed to another organisation without consent.	Information Sharing Agreements are being discussed to put in place with partners. Wherever possible and safe, consent is sought from participants to share their data prior to doing so. This is outlined on the ERMS Consent and Confidentiality form	Reduced	Medium	Yes
Participant refuses to sign form	An information sheet given to participants explains that the service may not be able to continue to work with a participant who does not sign the form. These forms sit on MyRJ as a "Closed Case"	Reduced	Medium	Yes
Illegitimate access to Police information	Only employed staff, who are vetted to management level and have completed training have access to ATHENA and PNC police systems.	Reduced	Medium	Yes

Step 7: Sign off and record outcomes		
Item	**Name/position/date**	**Notes**
Measures approved by:	S Humphreys DPO 02 September 2021	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	S Humphreys DPO 02 September 2021	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	S Humphreys DPO 02 September 2021	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
This DPIA will be kept under review by:	S Humphreys DPO	The DPO should also review ongoing compliance with DPIA