The DPIA is to be undertaken when you have completed a **DPIA Need Checklist** and been assessed by IMT as **requiring a DPIA**.

Your completed **DPIA Need Checklist** must be attached to this DPIA.

You may not have all the information right now, which is fine. This assessment will evolve through your planning, implementation and transfer to business as usual. Please mark a question N/A or nil if you feel it does apply to your project/process.

We encourage you to include/attach **process maps**, **data flow diagrams**, or **organisational relationship maps**, as these are a good way to explain a process. These can be hand drawn.

This process is for use of personal data, but be aware that non-personal data implications also need to be managed correctly, with adequate records retention, such as use of address gazetteer data or PSMA licensing, copyright material and IPR. Speak to the Information Management Team for advice.

Name of lead officer completing the assessment	Date
[redacted]	08/02/2021

Process or Project

1. Description of the planned activity

Prevent Case Management and Channel

The Channel Project and Prevent Case Management (PCM) is a community-based initiative which works with the police, local organisations, communities and the 'Prevent' strand of the Home Office Counter Terrorism Strategy 'Contest' to respond to concerns about individuals at risk of, or vulnerable to, radicalisation, that might lead to them becoming terrorists or supporting terrorism. These individuals may not have committed a criminal offence, but information held by police and statutory partners may raise concerns of extremism.

2. Is the processing novel or has anything similar been undertaken before? Will you be using any innovative technical or organisational solutions, like smart tech?

No. The Channel process is similar to other multi-agency case management processes. As with other community safety case management processes, the ECINS case management system is used to store information in relation to Channel cases.

3. Do you plan to carry out profiling on a large scale?

No.

4. Will you use systematic and extensive profiling or automated decisions to make significant decisions about people? Will you use profiling, automated decision making or special category data to make decisions about someone's access to a service, opportunity or benefit?

No.

5. Will you use children's personal data for profiling or automated decisions making; for marketing purposes; or for offering online services directly to them?

No.

6. Will you systematically monitor a public place on a large scale *eg CCTV*?

No.

7. Do you plan to combine, compare or match data from multiple sources *eg fraud prevention*?

Yes. As part of the case management process, information is gathered from multiple sources including the Corporate Anti-Fraud Team (CAFT), Barnet Homes, Children's Services, Adult Social Care, Youth Offending and external statutory service providers including the National Probation Service, London Community Rehabilitation Company and Barnet-Enfield-Haringey (BEH) Mental health trust. The information is gathered to support an accurate assessment of risk in terms of the referred individual's vulnerability to radicalisation so that an appropriate support plan can be developed to address the areas of risk and vulnerability.

8. Will you process personal data in a way that involves tracking individuals' online or offline location or behaviour *eg vehicle tracking or monitoring an individual's social media*?

No. Although individuals referred to Prevent undergo an assessment by SO15 (Counter Terrorism) Police Unit and as part of the assessment. Police will assess the referred individual's online activity and any crime-related history that may be relevant to the individual's risk and vulnerability.

9. Anticipated start data and duration of processing (ongoing if no set end date)

Ongoing.

Purpose & Benefits

10. What are the aims of the processing? What is the intended effect on individuals?

To provide the referred individual with support to reduce the risk of radicalisation. The support package is designed to divert the vulnerable individual away from violent extremism and terrorist-related activity.

11. Why are you planning to undertake this processing? What legislation requires/affects your processing?

The partners are processing the data in support of the Channel Duty (Section 36, Counter-Terrorism and Security Act 2015, amended by the Counter-Terrorism and Border Security Act 2019), whereby individuals vulnerable to being drawn into terrorism are referred to Channel Panels to be considered for support to reduce that risk. If partners did not have access to this information, the panel would not be able to make accurate and informed decisions on the risk of radicalisation and the actions necessary to mitigate these risks. This would impair the ability of the partners to meet their statutory duty to prevent vulnerable residents from being drawn into terrorism, for the protection of the data subjects and the wider public.

The government's statutory Channel guidance.

The Revised Prevent Duty Guidance states the following

(see https://www.gov.uk/government/publications/prevent-duty-guidance/revised-prevent-duty-guidance-for-england-and-wales)

Sharing information

The Prevent programme must not involve any covert activity against people or communities. But specified authorities may need to share personal information to ensure, for example, that a person at risk of radicalisation is given appropriate support (for example on the Channel programme). Information sharing must be assessed on a case-by-case basis.

There may be some circumstances where specified authorities, in the course of Prevent related work, identify someone who may already be engaged in illegal terrorist-related activity. People suspected of being involved in such activity must be referred to the police.

The lawful basis on which we collect and use your personal data is that 'processing is necessary for the completion of task carried out in the public interest.'

Law Enforcement processing

The work is not expected to lead to law enforcement action (and LE processing) because this is an early intervention project to reduce the risk of crime. During the process the police SO15 carry out a deconfliction process, as part of their gateway assessment, which checks that the individuals is not linked to any terrorist or criminal activity investigations, which reduces the chance that LE processing will be required.

12. What are the benefits to the individual, society and the organisation(s) involved?

The Channel Panel process will gather information about individuals referred and assess their vulnerability to being drawn into radicalisation that may lead to violent extremism. The purpose of the panel is to assess the level of risk and provide support to those deemed vulnerable in order to appropriately safeguard them from being drawn into terrorism.

There is a positive benefit to individuals, who are supported to avoid future criminal activity. There is positive benefit to society in supporting individuals into productive lives, and in reducing the risk of criminal and terrorist related activity.

13. What geographical area will the processing cover? *(This would generally be Barnet only, but your work may involve pan-London or national projects)*

Barnet, although information may be shared with other local authority areas if the vulnerable individual moves to a different area while still managed under Prevent Case Management / Channel processes.

14. Do you plan to consult with any person, group or organisation? Consultation can include a survey, public meetings or committee papers, market research or even a review of previous customer complaints.

We would seek to hold a community engagement event in the 2021-2022 calendar year but this would be designed to raise awareness of the Prevent duty. No personal information would be shared at any such event.

Individuals (data subjects)

15. What types of data subjects are involved? Tick all that apply.

- ☐ Customers or Service users
- ☐ Service providers / Contractors
- ☐ Residents
- ☐ Complainants
- ☐ Claimants
- ☐ Recipient of benefits
- ☐ Traders or people subject to inspection
- ☐ People captured on CCTV
- ☐ Representative of another organisation
- ☐ Licence and permit holders
- ☐ Employees (previous or current)
- ☐ Councillors, MPs, elected officials

☐ Volunteers

☐ Professional adviser or consultant (eg doctor or lawyer)

☒ Any

16. Are the data subjects considered vulnerable eg children or domestic abuse victims? What is the council's relationship with the data subject? Is there an imbalance of power, as with employees? How much control will data subjects have?

The information shared will be related to members of the public who have been referred to the Channel/Prevent programme:

- These individuals can be of any gender or race and can be children or adults
- These individuals can be of any age but where children are concerned it is unusual to receive a referral in isolation about children under the age of 7 due to the lack of mental capacity of the child to form an ideological perspective
- The majority of referrals to Channel are for vulnerable individuals (both children and adults).

We will process data on the individuals who relate to the person at risk of radicalisation, such as their family and friends, where this is relevant to the assessment of the referred individual's level of risk and vulnerability and the delivery of appropriate support.

Data subjects do not have control over the processing of their data.

17. Expected volume of data subjects *eg number of people or number of records*

Numbers vary. The caseload is relatively low in comparison to domestic abuse and anti-social behaviour MARAC panels. I would not expect more than 20 live cases at any time.

18. How is the individual being informed of the processing *(privacy notices)*? Do you plan to process personal data without providing a privacy notice *eg investigations or covert surveillance*?

A privacy notice will be developed and placed on the local authority website informing data subjects of the reasons why information needs to be processed and the need to share information with our partner statutory agencies in order to support vulnerable individuals at risk of being radicalised and in order to support the development of accurate risk assessments.

After initial assessment an approach is made and the process and use /sharing of data will be explained to the individual. At this stage those assessed will be informed of the Privacy Notice on the local authority website.

19. How do you plan to support the Rights of Data Subjects (*eg access to information*)?

Articles 13 and 14 of the GDPR require certain information to be provided to Data Subjects, including how their data is being processed, at the point of processing. This obligation will always apply except where the Controller is exempted from so doing by reason of exemptions in the DPA. Each exemption must be considered and recorded on a case by case base and not applied uniformly. Each Party shall ensure that, where relevant, it complies with Articles 13 and 14 of the GDPR in processing Personal Data, and/or Special Category Data and/or Criminal Conviction Data.

The lead referring agencies are expected to notify Data Subjects that they have been referred to Channel panel unless a specific exemption applies e.g.

- Providing the information to the individual would render impossible or seriously impair the achievement of the objectives of the processing - for example information disclosed relating to an ongoing investigation, may increase the safeguarding risks posed to the Data Subject etc.
- Obligation of professional secrecy regulated by law that covers the Personal Data disclosed – this may apply where for example another family member has raised concerns with social worker in confidence.
- National security - part of the Personal Data disclosed has been processed for the purposes of safeguarding national security or defence

20. Will your processing prevent individuals from exercising a right, or using a service or contract?

No.

Data

21. What type of information will be collected? Tick all that apply.

- ☒ Name
- ☒ Address
- ☒ Contact details
- ☒ DOB
- ☒ Equalities information
- ☒ Financial information
- ☒ Property information
- ☒ Social services information
- ☒ Human Resources information
- ☒ Employment
- ☒ Education information
- ☒ Housing information
- ☒ Family / relationship information
- ☒ Information from another local authority

☒ Criminal (allegation or prosecution) information
☐ Images in photographs, film or CCTV
☒ Health / Medical information
☒ Referral / Assessment information
☐ NHS number
☐ Referees
☒ Support network

22. Are you processing?

☒ Special category data
☒ Criminal / allegation offence data

Please specify.

Details in relation to a referred individual's race, ethnicity and gender are routinely recorded.

In cases where a referred individual is known to Police, Criminal / allegation offence data may be shared if this is relevant to the referred individual's risk and vulnerability to radicalisation.

23. Will you be processing biometric data? Please specify.

No.

24. Will you be using the above special category, biometric or criminal data on a large scale? Please specify.

No.

25. Is there a risk of physical harm in the event of a security breach *eg fraud investigations or child exploitation*?

It is possible that a security breach could, in some cases lead to a risk of physical harm.

26. How is the information being collected? Where are you getting it from?

Once a referral is received it is passed to the Met Police SO15 (Barnet) unit who carry out an assessment of the individual's vulnerability to radicalisation. SO15 Police will routinely send an Information Sharing Request (ISR) Form to the council's Prevent Coordinator for processing. This form is then sent to the Prevent Single Point of

Contact (SPOC) within Children's Social Care, Adults Social Care, Barnet Homes. Barnet Youth Offending Team, the National Probation Service, London Community Rehabilitation company (CRC) and the Barnet, Enfield, Haringey (BEH) mental Health Trust. Information regarding the vulnerable information is then collated by the Prevent Coordinator and then emailed securely to SO15 Police for assessment. Completed ISR forms are stored securely on the referred individual's ECINS profile.

27. Are you processing personal data for a different purpose than it was originally collected?

No.

28. Volume of data *eg number of records*?

Each referred individual who is assessed as suitable for the Channel process has a profile created on ECINS. I would not expect more than 20 live cases at any time. Where more than one individual is linked, a case is created linking both profiles.

29. How often will you be using the data *eg every day or annually*?

Data will be used regularly while the Channel case record is active, often more than once per week.

30. How is the information being stored, including backups, paper files in off-site storage, copies etc?

Channel Case records are stored in ECINS as described above.

31. How will you ensure good data quality? *eg regular checks or updating processes*

The Barnet Prevent Delivery Group meets quarterly and oversees the operation of Channel locally. This allows partners to discuss areas of concern in relation to the Channel process including information sharing processes.

32. What processes are/will be in place for editing or deleting information? We must be able to amend and fully delete personal data from systems.

Channel case records on ECINS are stored for 10 years after the case is closed to Channel (6 years after the completion of the 12 month review after case is closed to Channel). Once a case is closed to Channel, the case is archived on the ECINS case management system.

33. Are you using contractors/service providers to process the data?

The council uses the ECINS system from Empowering-communities. This is hosted by Empowering-communities (Empowering Communities provides a secure, GDPR compliant, cloud-based hosting of the system).

34. How is the information to be transported/transferred *(electronic and paper)*?

Where information is shared between agencies secure/encrypted email is used to send the information.

35. How will access to the data be managed and monitored *eg audit trails, logs*? Which officers/roles will have access to the asset?

The ECINS profile for each Channel case includes a log where actions in relation to each vulnerable individual are recorded on their profile.

36. What security measures will be in place?

Limited access rights as described below ensure that the information is stored securely: Access to Prevent/Channel ECINS profiles and cases are restricted to the Barnet Prevent Coordinator, Prevent Education Officer, Barnet Community Safety Managers and Barnet SO15 local Ops.

37. Are there are plans to store data outside the UK? Consider hosted sites, disaster recovery and IT support.

No.

38. Will reports be generated from this information, or statutory returns? If so, will the information be personally identifiable or anonymous?

Where data reports/information is provided in relation to Prevent / Channel casework all case information is anonymised so that referred individuals cannot be identified.

39. What is the retention period for this information? Consult the council's Retention Schedule. If your processing is not listed, contact recordsmanagement@barnet.gov.uk

Channel case records on ECINS are stored for 10 years after the case is closed to Channel (9 years after the completion of the 12-month review after case is closed to

Channel). Once a case is closed to Channel, the case is archived on the ECINS case management system.

40. What process is/will be in place to implement this retention period?

ECINS data will be reviewed on an annual basis and cases reaching the end of the retention period will be deleted manually.

41. What is the process for managing/transferring/destroying personal data during start-up and close down?

ECINS Case / profile records are deleted 10 years after the closure of a case to Channel.

42. If the organisation/service ceases, what will happen to the information?

Not applicable.

43. Can data be anonymised or pseudonymised? How will ensure you only use the minimum amount of data required to complete the aim?

Data can be pseudonymised in email communication between partners where possible.

44. Who do you plan to share information with? Tick all that apply

- ☐ DWP
- ☐ Council legal service
- ☐ Legal representatives
- ☒ Police
- ☐ Insurance companies
- ☒ Other local authorities
- ☐ Home Office
- ☐ Health agencies
- ☐ Ofsted
- ☐ Voluntary agencies / Third sector
- ☒ Housing providers
- ☐ Expert witnesses
- ☐ Professional regulatory bodies
- ☐ Trade unions
- ☐ Credit reference agencies
- ☒ UK Border Agency

☐ Judicial agencies eg Courts

☒ Prison / Probation services

☒ Other council services (specify below)
Family Services, Adult Social Care, Barnet Homes, Barnet Youth Offending Service,

☐ HMRC

☒ Specialist organisations (specify below)
Barnet-Enfield-Haringey Mental Health Trust (BEH)

☒ Government departments (specify below)
Home Office (Office of Security and Counter Terrorism)

45. What information is shared?

- personal information (name, DOB, ethnicity, address, telephone, email, NHS number, proof of identity, unique pupil number);
- parents/carers personal information;
- personal information about other members of household;
- personal information about close relatives;
- details of family relationships in and outside of the household;
- data subject and family's legal status;
- accommodation;
- employment status;
- details about physical and emotional well-being and parenting;
- details of any risk issues;
- youth offending information: offences (including alleged offences), criminal proceedings, convictions and sentences;
- medical history;
- mental health history
- health, social care or other services provided;
- information about situation given to us by family/carers and/or other organisations (e.g. GP, school nurse, Police);
- reports relating to situation (e.g. safeguarding and other assessments, Child Protection Plans and Looked After Children reviews);
- educational progress and attainment information;
- school attendance, exclusions and behavioural information; and
- information such as court orders and professional involvement;
- The data subject and immediate families' immigration history if relevant to the case (e.g. intelligence suggesting radicalisation / affiliation with foreign or transnational extremist or terrorist organisations);
- police audio and video recording;
- any documents sent to us relating to the data subject (e.g. referrals received from other agencies and professionals);

Special category information used when assessing the safeguarding concern can include:

- racial or ethnic origin,

- political opinions,
- religious or philosophical beliefs,
- data concerning health,
- sex life / sexual orientation

Risks

46. Are there any known information risks, issues or public concerns? Has there been press interest or court cases relating to this type of processing?

None that I am aware of. The national Prevent Duty has however come under considerable scrutiny and criticism in the national media. It is therefore highly likely that any information breach would attract considerable attention from certain media outlets and community based organisations.

47. Any known activities and risks that will have a direct effect on this piece of work?

No.

Risk Table

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** Remote, possible or probable	**Severity of harm** Minimal, significant or severe	**Overall risk** Low, medium or high	**Options to reduce or eliminate risk**	**Effect on risk** Eliminated reduced accepted	**Residual risk** Low medium high	**Measure approved** Yes/no
Information Security breach.	Remote	Significant	Low	Information is stored securely on the ECINS case record system. Each Prevent profile (case record) has significant access rights restricted to the Prevent Coordinator, Prevent Education Officer, Barnet Community Safety Team managers and Barnet SO15 local Ops Police Unit. Information is shared via encrypted//secure email to avoid breach.	Reduced	Low	Yes
Vulnerable individual or family member speak to the press or anti-Prevent lobby groups complaining about Barnet Prevent related processes.	Possible.	Minimal.	Low.	Risk cannot be eliminated. The Barnet Prevent team have strong links with the legal and communications teams in the local authority and the Met Police SO15 Unit would be informed and engaged around any emerging situation to develop a communications' strategy to address any criticisms.	Reduced.	Low.	Yes.

Approval

DPO advice provided by:	[redacted]	Date: 15/02/21

DPO advice:

The personal data being processed is sensitive and about vulnerable individuals, so strong controls are required. There is a suitable lawful basis for this work and the processes described in this DPIA provide suitable safeguards.

The service must ensure that those working with and sharing the data keep the sensitivity of the data at the forefront of their minds.

The Prevent work requires privacy notices and an information sharing agreement, along with process documents for staff. A revised information sharing agreement is in progress as part of a project on pan-London data sharing.

Documents the service is required to complete/update:

- ☒ Privacy Notice
- ☒ ISA
- ☒ Process documents
- ☐ Other (specify below)
- ☒ ROPA
- ☐ Contract / DPA
- ☐ Internet pages/links
- ☐ Procedure for data subject requests

ICO advice sought	Date requested:	Date received:

ICO advice:

N/A

SIRO advice sought from:		Date:

SIRO views (Reasoning if differs from DPO advice): N/A		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by: [redacted]	Date review to take place: 01/02/2023	Date DPIA Agreed: 17/02/21