ORG OPEN RIGHTS GROUP

OPEN RIGHTS

PREVENT AND THE PRE-CRIME STATE: HOW UNACCOUNTABLE DATA SHARING IS HARMING A GENERATION

ABOUT ORG

Open Rights Group (ORG) is a UK based digital campaigning organisation working to protect fundamental rights to privacy and free speech online. With over 40,000 active supporters, we are a grassroots organisation with local groups across the UK.

We believe technology should be harnessed for social good and oppose repressive policies that exacerbate racism and discrimination and undermine people's right to be presumed innocent.

Our work on data protection and privacy includes challenging the immigration exemption to UK data protection law, defending the General Data Protection Regulation (GDPR) from attempts to water down its provisions, and challenging uncontrolled and unlawful data sharing by online advertisers.

openrightsgroup.org

Figure 1 Image derived from James Paget University Hospitals Prevent Policy (see Annex A); published as fair dealing, news reporting, criticism and review. Copyright may subsist in the original document.

Figure 2 Graphic of Data flow of Prevent decision making process from an original graphic by Charlotte Heath-Kelly, cc-by-sa.

Figure 3 Image derived from Prevent referral flowchart demonstrated by the City of London. Source: City of London Prevent Policy. Published as fair dealing, news reporting, criticism and review. Copyright may subsist in the original document.

PREVENT AND THE PRE-CRIME STATE:
HOW UNACCOUNTABLE DATA SHARING IS HARMING A GENERATION

EXECUTIVE SUMMARY

When Sami was six years old, his personal data was held in a database controlled by Counter-terrorism Police, accessible to local forces through myriad other systems. For what reason could a six-year-old boy be of interest to Counter-terrorism? The reason was that his father refused to engage with Prevent – the arm of the UK's counter-terrorism strategy existing within pre-crime territory i.e. trying to spot the terrorists before they become them.

The idea that such a young child could be singled out as a would-be terrorist was as ridiculous to the courts as it was to any reasonable person – even his father who caught the ire of the police was not involved in any crime. However, it took perseverance from the child's parents to successfully get Sami's data removed from the main Prevent database. Still, they couldn't guarantee that his personal information wasn't still lurking on other systems with other police forces; clearing Sami from the pre-criminal space would take a tracing exercise to find out who held his data and making an individual request with each party to remove it.

If the retention of Sami's data sounds unnecessary and the efforts to remove it seem disproportionate, then know that such a practice is incompatible with the UK's data protection regime. However, the Prevent Duty essentially mandates this practice nationwide with referrals coming from educational institutions, healthcare and other public authorities as well as police. The idea is that individuals should be referred to Prevent if they are showing signs of radicalisation and if they meet a threshold defined by section 36 of the Counter-terrorism and Security Act 2015, and if they agree, the individual can undertake an intervention under the Channel programme that assists in their deradicalisation via a multi-agency process.

The idea may seem like a genuine attempt at deterring terrorist activity but the reality is that many of the individuals referred will never warrant an intervention as they render no objective radicalisation or terrorism threat. By the time authorities agree that no threat exists, referees are already logged on the system, are not automatically removed and as a matter of course, their data is shared on to several other systems.

Prevent referees are not charged with an offence yet their lives are subject to scrutiny. And thousands are vulnerable to an unlawful and parallel infringement of their information rights. This incursion is compounded when the Prevent referee does not go through the multi-agency Channel process but is instead managed under a police-led process, where national security exemptions can be applied to limit rights to rectification, access and removal. Sitting within this covert space, the question becomes what oversight and parliamentary scrutiny is there of data sharing, processing and storage within Prevent.

Open Rights Group, with support from Prevent Watch and Lewis & Klein Associates, have looked at case studies, policies and guidance supplied in the public domain and through freedom of information (FOI) requests and outlined a snapshot of how data is retained, stored and shared under Prevent. From the information gathered, it appears that the retention of referees' data lacks a policing purpose. Often, the reason for a referral does not warrant a Prevent referral being made at all and the authorities have no choice but to render there to be no further action (NFA) with such NFA cases making up the vast majority of referrals.

These cases are left on systems for at least six years and for up to 100 years. However, these retention periods align with operational guidance that was not designed for pre-

crime. Such excessive retention periods are neither necessary nor proportionate to the standards required under UK data protection regulations. And when it comes to Prevent and the sensitive data involved, the highest thresholds of proportionality are needed.

Not only are the grounds to retain Prevent data insufficient but it is also important to note that the policy's implementation means information is shared between databases and agencies, between regional authorities, with national government policy teams and could be shared overseas. The lawful basis for sharing data under Prevent is statutory, as guidance indicates that gaining consent – another potential lawful basis for sharing data – from individuals may be problematic. In many instances, people do not know they have even been referred.

While the main legislation cited as providing the statutory basis is the Counter-Terrorism and Security Act 2015, several other statutes may be relied on to share data, each with potentially different thresholds for lawful processing. Yet, there is no guidance around how Prevent data is treated according to which statute or lawful basis.

Data could be held at every point of the referral system, including by the referring institution. Within the Counter-Terrorism Policing Prevent team alone, data could be copied to several databases. Any or all of these systems could have separate retention, deletion and review schedules, while factors determining removal are subjective and it is unknown if removal from one system will trigger removal from all the systems.

There are risks of onward sharing and processing from third-party partners and lack of guidance or agreements means the parameters within which such sharing can legally occur are not clearly laid out. If guidance or agreements exist, they may differ between regions and agencies and at the end of it all, the decision to share the information boils down to a subjective assessment of whether sharing is necessary. The extent to which a person's data is processed is unknown to that subject and potentially harms their life chances, including educational opportunities.

In one case involving a 17-year-old boy called Munir, the student's sixth form received his secondary school safeguarding file with information on his Prevent referral. So, when Munir got in trouble for breaching the dress code by wearing his Islamic dress outside of agreed Friday prayer times and discontinued an A level that he felt was antithetical to his views as a Muslim, the school accused him of not having inclusive values with the Prevent referral to reinforce this view. The debacle impacted his schooling.

There are other educational institution bilateral sharing agreements including between further and higher educational institutions, therefore, the offer of a university place can also hinge on whether a pupil received a Prevent referral, even if it was deemed NFA.

As this report shows, the sharing of Prevent data with airports, ports, immigration services and numerous other databases, means that some Prevent referees could be impacted in any facet of their life where they have contact with authorities.

If data processed and stored on police databases is not a complicated reality itself, there are other potential systems within the local authorities where retention and storage of data are subject to separate guidelines. And there is generally a dearth of guidance on how bodies will comply with a person's right to have their data erased.

When a person's data is shared with more than one body, they have the right to know who it has been shared with and to have that data removed. That right would need to be exercised with each organisation individually i.e. the data subject would first need to establish with whom data was shared and to issue each body with a request to get it removed. It therefore, becomes too onerous for an individual or their family to exercise their data protection rights – the right to object, rectification or erasure – which often requires legal action at personal expense.

Success in the courts for removing Prevent referral data has shown that the lawful basis for retention can be easily questioned where the resources and capabilities to challenge

exist. At one point 95% of Prevent cases did not meet the thresholds for any terrorism or radicalisation threat, so how can retaining all that data have a lawful purpose?

We believe that success stories in the courts would multiply if there was more transparency about when referrals are taking place and with whom. That transparency should extend to information requests, including personal subject access requests by individuals subject to Prevent.

The current system around Prevent denies rights, criminalises individuals without an offence in the frame and can potentially discriminate against individuals. What's more, legislative changes will hand more power to state institutions while weakening safeguards.

Over the last five years, annual referral figures have shown more Prevent referrals classified as 'Extreme Right Wing' than 'Islamist'. However, in last year's Review of Prevent by William Shawcross called for more focus on Islamist extremism. Given the reported rise in referrals since the escalation of the crisis in Israel and Gaza, Shawcross's recommendation could lead to the disproportionate targeting of Muslims and further surveillance of this already marginalised community.

Open Rights Group is making the following recommendations:

1. The government scraps the Prevent Duty to free resources to focus on evidence-based counter-terrorism strategies rather than speculative pre-crime guesswork; it should impose an immediate moratorium on Prevent referrals.
2. The Home Office imposes a blanket ban on the retention of data where thresholds under section 36 of the Counter-terrorism Act are not met.

Should the government fail to scrap Prevent and the Home Office continues to retain data even where thresholds are not met, we recommend:

3. The ICO audits the Home Office's Prevent policy and its execution across the various institutions where the processing of personal data takes place, including the applicability of national security exemptions, applied when Prevent falls under a police-led process.
4. The ICO directs data controllers of the Prevent programme to provide guidance to ensure data subjects can track where a Prevent referral has been made for them to execute their right of erasure.
5. Policing bodies review the management of information related to Prevent with stricter deletion rules where there has been no further action.
6. Local authorities, police departments and individual institutions subject to the Prevent duty ensure maximum transparency around referrals, data processing and data sharing practices, including the systems used and in as clear detail as possible.
7. The NHS should ensure that there is no onward sharing of Prevent-related data on other platforms and that data is not reused for other purposes.
8. Statistics (aggregated data) should be transparently published to enable scrutiny and support accountability.
9. Data about the number of Prevent referrals, amount of information held and outcomes of referrals should be available on a geographic level to support with demographic information and scrutiny of the programme.
10. The Prevent programme should publish data flows to help people understand how to use their information rights.
11. A clear route for complaints and requests for deletion or review should be put in place
12. Notification of people whose data has been held in the Prevent system but subsequently removed should take place.
13. Guidance to those under the duty should specifically notify them that referrals are passed to intelligence officers for the initial Prevent Gateway Assessment and data is therefore processed in the covert space.

14. Where a decision data crosses a threshold from safeguarding to crime use, or from police to national security use, an independent authority should decide whether the data is to be shared, rather than the decision being an internal police matter. The principle of independent decisions for data use already exists regarding Communications Data under the IPA for example.[1]

We hope that this report will encourage others to continue to challenge the abrogation of rights occurring under the Prevent policy, including that:

15. Members of the legal community conducts a legal challenge to the lawfulness of the Prevent Duty and its infringements on UK data protection law and Article 8 of the Human Rights Act 1998 – the right to privacy.

16. Individuals should submit subject access requests to determine if they or their child has been referred under Prevent and exercise their right to object, rectification and erasure.

17. Individuals refused their rights escalate their request through the ICO complaint mechanism, a Department of Education complaint, tribunal or judicial review.

18. Researchers should map the data collection, retention, storage and sharing practices of local areas to determine compliance with data protection laws.

The government and political opposition should review Open Rights Group's recommendations around the Data Protection and Digital Information Bill and should support dropping the bill or engaging the amendments to improve safeguards for those entangled in the UK's pre-criminal space.

INTRODUCTION: PRE-CRIME AND PREVENT IN THE UK

The term 'pre-crime' may sound like it belongs solely in the pages of dystopian fiction, popularised by the 2002 film *Minority Report* based on Philip K. Dick's 1956 science fiction novella. However, the principle dates back to the 19th century when criminologists theorised that it was possible to recognise criminals before they committed any crime. Fast forward to the 21st century and we're seeing it applied in practice by law enforcement and other public services.

One of the most prevalent policies that embodies the pre-crime principle is the Prevent Duty – one prong of the government's counter-terrorism strategy CONTEST[2] that aims to divert people from becoming radicalised before they could possibly commit a terrorist offence. The framing of Prevent as sitting in the pre-criminal space has even appeared in National Health Service (NHS)[3] and local authority guidance[4] for staff, taking it from fantasy to fact.

Pre-crime and pre-crime initiatives, such as Prevent, are controversial, as they undermine the right to be presumed innocent, one of the fundamental tenets of most criminal justice systems. This tension has not prevented increased use across Europe and the US in recent years. At the same time, there has been growing public awareness of the racism and discrimination that is inherent within policing and criminal

1 https://www.legislation.gov.uk/ukpga/2016/25/part/3 and https://www.legislation.gov.uk/uksi/2018/1123/regulation/5

2 The four arms to CONTEST are prevent: to stop people becoming terrorists or supporting terrorism; pursue: to stop terrorist attacks happening; protect: to strengthen our protection against a terrorist attack; and prepare: to minimise the impact of a terrorist attack.

3 Goldberg, D, Jadhav, S, Younis, T (2017). Prevent: what is pre-criminal space? National Library of Medicine > National Center for Biotechnology Information https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5537575/

4 Bedfordshire, Luton and Milton Keynes Health and Care Partnership Safeguarding – Adults and Children Policy (Annex A); Barking & Dagenham, Havering and Redbridge (BHR) Primary Care Safeguarding Handbook (Annex A).

justice systems.[5] Yet these institutions are running programmes to determine who is likely to commit a crime, in some cases based on decisions formed from people's background, education or ethnicity, or where they live and who they know or live with.

These presumptions can have very harmful real-life consequences for affected individuals, including being searched, placed under surveillance, detained without charge and threatened with having their children removed. Unsurprisingly, given that they often rely on flawed data, such programmes have been shown to reinforce existing discrimination within criminal justice and further alienate marginalised communities.[6]

In the UK, pre-crime strategies can involve disruption to a person's life such as involvement of social services, restriction of freedoms such as curtailing free speech, control orders and detention without charge. Although these tactics are familiar in the counter-terrorism space, they have become increasingly prevalent in other areas of policing. UK legislation that gained Royal Assent in 2022-2023 and that gives the police pre-crime powers include the Public Order Act, which has introduced Serious Disruption Prevention Orders allowing bans on protesting,[7] and the Police, Crime, Sentencing and Courts Act, which expands the tools and powers available to the police to 'prevent crime,' such as the extraction of digital information from electronic devices.[8]

The Prevent Duty

The Prevent Duty, which sits within the Counter-Terrorism and Security Act 2015, section 26,[9] states that certain bodies must have "due regard to the need to prevent people from being drawn into terrorism." For over a decade, numerous civil society groups, human rights organisations and UN special rapporteurs have raised concerns about the human rights breaches of Prevent. This report uses Prevent as an example of pre-criminal legislation to demonstrate the specific dangers to data rights.

The policy itself has evolved[10] from a focus on projects aimed at community integration to a whole-of-society and institutional approach, and now all providers of public services, also named in the Act, have a duty to report behaviour they believe suggests a vulnerability to radicalisation. The reported behaviour and possible referral are based on a subjective assessment; if, under further scrutiny, the concerns are deemed "justified," the referral can escalate to the Channel panel, which will decide whether the individual should be subjected to interventions to "de-radicalise" them, as per section 36 of the Counter-Terrorism and Security Act 2015.

These duties have notably been imposed on health services, teachers and social workers and, particularly, educational institutions, where most referrals have occurred. On the face of it, that fact may seem to suggest that schools and universities are forming a hotbed of radicalisation but

5 Racism in Europe's law enforcement and criminal justice systems. Fair Trials (2022) https://www.fairtrials.org/app/uploads/2022/06/2022-05-20-evidence_racial_injustice_final.pdf; Systemic racism within UK criminal justice system a serious concern: UN human rights experts https://news.un.org/en/story/2023/01/1132912

6 Eroding Trust: The UK's Prevent Counter-Extremism Strategy in Health and Education. Open Society Justice Initiative (2016) https://www.justiceinitiative.org/publications/eroding-trust-uk-s-prevent-counter-extremism-strategy-health-and-education

7 Public Order Act: Serious Disruption Orders (2023). Liberty https://www.libertyhumanrights.org.uk/advice_information/public-order-act-serious-disruption-prevention-orders/#:~:text=Part%202%20of%20the%20Public,anything%2C%20described%20in%20the%20order.

8 Brief: Issue 10 (2022). College of Policing https://assets.college.police.uk/s3fs-public/2022-11/College-of-Policing-Brief-November-2022.pdf

9 Counter-Terrorism and Security Act 2015, Part 5, Chapter 1, Section 26. Legislation.gov.uk https://www.legislation.gov.uk/ukpga/2015/6/section/26/enacted

10 Thomas, P (2020). Britain's Prevent Strategy: Always Changing, Always the Same? Palgrave Macmillan https://link.springer.com/chapter/10.1007/978-3-030-45559-0_2

what is concerning is that the majority of referrals[11] are never progressed, either subsumed under other safeguarding interventions or deemed insignificant enough to drop, by Prevent's own logic.

This high rate of what Medact calls "false positives"[12] sheds light on the policy's utility or lack thereof. But even if a referral is not progressed, that is not the end for those affected: those referrals remain in police, local authority and government systems in line with retention periods for genuine safeguarding issues and protocols determined for criminal issues. In fact, most people do not realise that referring an individual places that individual's data directly with the security services as well as potentially onto local authority and multi-agency partners.

At the sharp end of Prevent referrals are people fed through the system via their personal data – collected, retained and shared, yet seldom removed – causing harm and impeding rights. In 2019, FOI requests submitted by Liberty revealed that data was being retained on the Prevent Case Management database, which is managed centrally by national Counter-Terrorism Policing headquarters–.[13] but the reality is that is one of many systems where their data is stored and linked to Prevent.

IN THE UK, PRE-CRIME STRATEGIES CAN INVOLVE DISRUPTION TO A PERSON'S LIFE SUCH AS INVOLVEMENT OF SOCIAL SERVICES, RESTRICTION OF FREEDOMS SUCH AS CURTAILING FREE SPEECH, CONTROL ORDERS AND DETENTION WITHOUT CHARGE

While most people in the UK enjoy robust data protection standards, those rights look very different for people referred under the Prevent duty. We will show through this report that:

- The processing of personal data under Prevent amounts to unfair processing and does not meet the requirements of necessity and proportionality.
- There is no valid policing purpose for retaining the personal data of most Prevent referees.
- There is a conflation of 'victim' and 'perpetrator' in justifying individuals' referrals under Prevent.
- The pathway of Prevent an individual is steered onto – police-led partnership or multi-agency process – determines the application of different data protection standards for removal, rectification and access.
- There are gaps in guidance as to what type of threshold must be met according to the lawful basis for sharing personal data and when that data is removed.
- Data sharing without consent has risks and long-term impacts for the individual concerned.
- The right to erasure – a key data right – is rarely afforded and can be readily disregarded if too much onward sharing has taken place.
- A Prevent referee's access to their rights to object to their data or have it rectified or erased is too onerous often requiring legal action at personal expense.
- Prevent processes are opaque and organisations are liberally invoking national security and law enforcement exemptions to avoid disclosing information.
- The power imbalance between state and individual will only weigh more heavily in favour of the former as new legislation kicks in.

11 87% according to the 21/22 statistics published by the Home Office but it had been 95% for several years consistently before that

12 False Positives: the Prevent counter-extremism policy in healthcare (2020). Medact https://www.medact.org/2020/resources/reports/false-positives-the-prevent-counter-extremism-policy-in-healthcare/

13 Liberty uncovers secret Prevent database (2019). Liberty https://www.libertyhumanrights.org.uk/issue/liberty-uncovers-secret-prevent-database/

Open Rights Group has worked with Prevent Watch, the key watchdog on Prevent, and researchers Lewis & Klein Associates to explain how personal data is collected, retained and shared under Prevent and how this processing meets data protection standards.

The findings will outline how the referral mechanism works across different phases of the process, what legal justifications are used to share and process this private data and what data sharing agreements could be in place to ensure the seamless transfer and processing of the data. We also illustrate the invasive nature of Prevent referrals, their harms and the divergence from protocols most Britons enjoy. Finally, we lay out the changes in the law that could impact the trajectory of data protection in the UK, which are set only to weaken the protections that exist.

Methodology

The data for this report was collected using a comprehensive online search of publicly available information, e.g. public information sharing agreements, privacy notices, data sharing guidance documents, etc. This online search was followed by FOI requests to authorities in England and Wales. The findings are based on 56 disclosures, which provide a snapshot of how the government, the police, local authorities, universities and the NHS share data when making referrals under the Prevent Duty.

Using FOI requests to establish information and retrieve documentation can be lengthy and vulnerable to evasive responses. The challenges of using them in terrorism research are compounded by successive governments who eschew transparency and the use of national security exemptions provided by the Freedom of Information Act 2000 to block requests.[14] These exemptions can, of course, be challenged, often successfully,[15] but the process can be time-consuming and seriously delay research.

Where FOI requests have been used and been successful, they have revealed how the Prevent Duty has conflated counter-terrorism and safeguarding introducing further bureaucracy.[16] Recent findings demonstrated the continued value of FOI requests to explore the functioning of counter-terrorism policy including the Prevent Duty.[17]

This report relies on FOI requests to understand how Prevent data is shared between organisations and to find out what happens with the data collected once a Prevent referral has been made. Before writing the FOI request, Lewis & Klein Associates spoke to practitioners in their extended network to understand what information is held and what specifically to request. The preliminary research allowed specific FOI requests to be drafted to minimise refusals.

The report also uses case studies that were sourced from Prevent Watch. These were cases where the individual had highlighted data processing as a major concern.

The report was also reviewed by members of Open Rights Group's Advisory Council and Charlotte Heath-Kelly, Professor of Politics and International Studies at University of Warwick.

14 Corderoy, J (2023). A Year after Partygate, Why Is the Government Still Being so Secretive? OpenDemocracy https://www.opendemocracy.net/en/partygate-cabinet-office-cctv-conservative-party-boris-johnson/; ICO (2023). When Can We Refuse a Request for Information? https://ico.org.uk/for-organisations/guide-to-freedom-of-information/refusing-a-request/

15 Institute for Government (2017). Freedom of Information: What Is Freedom of Information and Why Is It Important? https://www.instituteforgovernment.org.uk/explainer/freedom-information

16 Whiting and others (2020). The Prevent Duty in UK higher education: Insights from freedom of information requests. The British Journal of Politics and International Relations https://journals.sagepub.com/doi/abs/10.1177/1369148120968520

17 Ibid.

THE UK LEGAL FRAMEWORK FOR DATA PROTECTION

The legal framework for UK data protection is spread across multiple pieces of legislation. The main law is the General Data Protection Regulation 2016 ("UK GDPR") which was retained[18] when the UK left the EU and amended by several pieces of secondary legislation,[19] including the Data Protection Act 2018[20], which means these two statutes should be read together.[21] In its current form, UK GDPR is considered to be one of the strongest data protection regimes globally.[22] Like the EU's GDPR, the UK equivalent provides extensive rights to individuals, allowing them a greater understanding of and control over their personal data.

UK GDPR places protections on personal data, which is defined as any information that allows a living person to be directly or indirectly identifiable. This data includes a person's name, location or online username. It can also include less obvious information like a person's IP address and cookie identifiers.[23] UK GDPR also identifies several 'special' categories of sensitive personal data that are provided stronger protection: a person's racial or ethnic origin, political opinions, religious beliefs, sexuality, trade union membership status, genetic or biometric data and health information.

Necessity and proportionality

Under UK GDPR, individuals, organisations and companies that exercise control over personal data are known as 'controllers' or 'processors.' As such, they are accountable for ensuring two key fundamental principles regarding data processing: necessity and proportionality. These principles mandate that processing operations, retention periods and the categories of data processed are necessary – and proportionate – only for the purpose of the processing. Anyone processing or controlling a Prevent subject's personal information must therefore, keep the following principles in mind:

1. **Lawfulness, fairness, and transparency** – The processing information should be on grounds based on law, conducted in a way people reasonably expect without unjustified adverse effects and be communicated to the individual in an accessible manner.
2. **Purpose limitation** – There should be a clear purpose to the processing of personal data from the start. Data can only be used for a new purpose if it is compatible with the original purpose, new consent is given or there is a clear obligation in the law.
3. **Data minimisation** – Organisations should identify the minimum amount of data needed for their purposes and collect no more than that.
4. **Accuracy** – Controllers must take "all reasonable steps to ensure" that personal data is up to date and not incorrect or misleading, including correcting it, erasing it, clearly marking it as a mistake and responding to challenges to its accuracy.

18 European Union (Withdrawal) Act 2018. https://www.legislation.gov.uk/ukpga/2018/16/contents/enacted

19 The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019. https://www.legislation.gov.uk/ukdsi/2019/9780111177594/contents

20 Data Protection Act 2018. https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

21 Procurement Policy Note – Updated Guidance on Data Protection Legislation (2022). Cabinet Office https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1121141/Procurement-Policy-Note-03_22-Updated-Guidance-on-Data-Protection-Legislation.docx.pdf

22 Burgess, M (2020). What is GDPR? The summary guide to GDPR compliance in the UK. Wired https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

23 Ibid.

5. **Storage limitation** – Organisations should not keep data longer than necessary and justify the period they wish to keep it for. They should also review the data held periodically and erase it when no longer needed or asked to do so.

6. **Integrity and confidentiality (security)** – Organisations must have appropriate security measures in place to protect the personal data they hold.

7. **Accountability** – Organisations are responsible for handling personal data and compliance with data protection law and must have appropriate measures and records in place to demonstrate compliance.

Assessing risks and rights

In addition, controllers must complete a data protection impact assessment (DPIA) to help them identify and minimise the data protection risks of a project. This process is mandatory where processing will likely result in a high risk to individuals. Organisations are encouraged to complete a screening checklist to help determine if a DPIA is required but it is generally considered good practice for any major project.

BOX 1

DATA PROTECTION IMPACT ASSESSMENT

Guidance from the Information Commissioner's website[24] states that a data protection impact assessment must:

- **Describe the nature, scope, context and purposes of the processing.**
- **Assess necessity, proportionality and compliance measures.**
- **Identify and assess risks to individuals.**
- **Identify any additional measures to mitigate those risks.**

The level of risk is determined by the likelihood and severity of harm to individuals. The ICO states that high risk indicates "a high probability of some harm" or "a lower possibility of serious harm."

Consultation should be sought from the organisation's data protection officer, individuals, and relevant experts, as well as the ICO if a risk that can't be mitigated is identified.

When an individual's personal data is processed, the UK GDPR affords them key rights. The following are worth mentioning regarding those who have been referred under the Prevent Duty:

The right to be informed – Everyone has the right to be informed how and why their data is being collected and used, including purposes, how long the data will be held for and who it will be shared with; this privacy information should be provided immediately or within one month if obtaining it from other sources.

The right of access – Individuals have the right to access a copy of their personal data by submitting a Subject Access Request (SAR).

24 Data protection impact assessments. ICO https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-impact-assessments/

BOX 2

SUBJECT ACCESS REQUESTS

Individuals have the right to request a copy of the personal data held about them by an organisation through a Subject Access Request (SAR).

SARs help people understand what data an organisation is holding about them and how and why their data is being used. SARs also help people check if their data is being handled lawfully. Individuals can make SARs verbally or in writing, including via social media or online portals. The ICO states that organisations must comply with SARs "without undue delay and at the latest within one month of receiving the request."

More information about SARs can be found on the ICO website: **https://ico.org.uk/for-the-public/your-right-to-get-copies-of-your-data/**

The right to erasure, to object and to rectification – The three rights are similar and essentially entitle individuals to have their personal data erased, subject to limited processing or corrected, especially when the seven principles mentioned above have been undermined.

Key exemptions

The rights individuals have to privacy under the data protection regime are not absolute and at times authorities may conduct a balancing exercise against the right to privacy.

Prevent's position within a national security framework means that the UK's data protection regime carves out exemptions or entirely separate areas of law for the processing of data for law enforcement or national security purposes.

Law enforcement

The processing of personal data for law enforcement purposes is governed by Part 3 of the Data Protection Act 2018 and affords processing for the prevention, investigation, detection or prosecution of criminal offences. Data processing for these purposes is governed by six separate principles:[25]

1. **Processing of personal data for any of the law enforcement purposes must be lawful and fair.**
2. **The law enforcement purpose for collecting personal data must be specified, explicit and legitimate, and personal data collected must not be processed in a manner that is incompatible with the purpose for which it was originally collected.**
3. **Personal data processed for any law enforcement purpose must be adequate and relevant and must not exceed the purpose for which it is processed.**
4. **Personal data processed for any of the law enforcement purposes must be accurate and up to date with every reasonable step taken to ensure that inaccurate data related to the law enforcement purpose is erased or rectified without delay.**
5. **Personal data processed for any law enforcement purpose must be kept for no longer than is necessary for the purpose for which it is processed. Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.**
6. **Personal data processed for any law enforcement purpose must be done ensuring its appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.**

25 Information Commissioner's Office. Guide to Law Enforcement Processing > Principles https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/principles/

Limits to law enforcement processing can also be found in case law. For example, in *S and Marper v United Kingdom* [2008] ECHR 1581, the judge ruled that the blanket retention of biometric data for persons only suspected of offences was in breach of Article 8, paragraph 2 of the European Convention on Human Rights – the right to private life.[26]

National security

The exemption for general processing of data often invoked is section 26 of the Data Protection Act 2018, which sets out a broad exemption from key data protection safeguards "if exemption from the provision is required for (a) the purpose of safeguarding national security, or (b) defence purposes."

Processing children's data

The processing of children's data also requires careful scrutiny. Data protection law and the ICO place particular emphasis on protecting children's privacy, as children may be less aware of the risks, consequences, safeguards and their rights in relation to the processing of their personal data. That is why the UK GDPR requires that children are addressed in clear and easily understandable language during discussions related to data collection and retention.[27]

Critically, the law states that the right to have personal data erased is particularly important when processing is based upon the consent of a child. If a child cannot legitimately give consent then someone with parental authority over that child must give consent. If an organisation accepts consent from a holder of parental responsibility, they must include information that lets a child know they have a right to withdraw their consent once they are competent in any privacy information provided.

BOX 3

THE INFORMATION COMMISSIONER'S OFFICE (ICO)

The Information Commissioner's Office (ICO) is the UK's independent, regulatory body that promotes information rights in the public interest. It is staffed by over 500 employees with an annual budget of £85 million and its mission is to promote openness by public bodies and data privacy for individuals. The ICO has substantial powers to hold the government and businesses to account by imposing monetary penalties, conducting audits and offering advice and guidance. Consumers can make a complaint directly to the ICO if they believe their data is being misused.

26 A case summary can be found at https://docs.google.com/document/d/1T4NwyOX2ReiScckQ6AqXeoP_ynUsiSCcIR2lSu6hzrI/edit#heading=h.mebfrdrqcaw0. A full judgment can be found: European Court of Human Rights. Case of S. and Marper v. the United Kingdom (2008) https://hudoc.echr.coe.int/eng#%7B%22dmdocnumber%22:%5B%22843941%22%5D,%22itemid%22:%5B%22001-90051%22%5D%7D

27 The UN has also raised how the targeting of children must stop: CRC/C/GBR/CO/6-7 Committee on the Rights of the Child – Concluding observations on the combined sixth and seventh reports of the United Kingdom of Great Britain and Northern Ireland (June 2023). Office of the High Commission of Children's Rights https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GBR/CO/6-7&Lang=en

The future of the UK's data regime

It is worth noting that there are proposed changes to the country's data protection regime through the Data Protection and Digital Information (DPDI) Bill introduced in March 2023. These changes will weaken data rights, water down accountability requirements, reduce the independence of the ICO and empower the Secretary of State with undemocratic control over data protection.[28] Several changes in particular will further exacerbate the negative data environment surrounding Prevent:

- New exemptions for 'national security' and 'crime prevention' making it harder to challenge the government's retention and repurposing of data.
- Changes to Chapter 3 Data Subjects Rights that allow controllers to refuse data subject rights if they determine the request is 'vexatious or excessive,' including the right of access (SARs), right to erasure and the right to object to processing.
- Changes to rules around DPIAs, reducing the requirements to conduct one before processing people's data and removing the requirement to consult with individuals who might be impacted by the use of their data.
- New government powers over the ICO mean the Secretary of State would be able to issue instructions to the ICO and interfere with how the regulator functions.
- Changes to international data transfers will empower the Secretary of State to approve international data transfers to countries where data protection is limited and national security bodies operate with little data protection oversight.

DATA GATHERED DURING THE PREVENT PROCESS

Since 2015, there have been more than 51,000 Prevent referrals.[29] Prevent referrals are the core process by which persons enter the Prevent programme. Prevent is not self-referred; instead, people who have a concern about someone else will pass that person's information to Prevent. The Home Office programme consists of Prevent officers who sit within the counter-terrorism police force and partner with the local authority and other services such as schools, community groups, health practitioners and faith leaders.

A Prevent referral starts off as an unofficial report around someone's behaviour within one of the bodies listed in Schedule 6 of the Counter-terrorism and Security Act 2015,[30] which is discussed and considered by that body's safeguarding team and potentially, a local Prevent official. Whether or not the behaviour is considered significant, it may still be recorded within internal systems. It may be rejected at this stage or be referred to a local, multi-agency Prevent panel, which is when data on referrals is gathered.

Once a referral is received by Prevent it will be assessed in coordination with these partners to see if the concern is such that the individual requires an intervention via the deradicalisation programme called Channel.

This journey of being considered for a Prevent referral, through to being considered and potentially adopted as a Channel case, involves several multi-agency partners (e.g. local authority children's services, education

28 Data grab bill will set back the UK economy and rights: Briefing on the Data Protection and Digital Information (No 2) Bill. Open Rights Group https://www.openrightsgroup.org/publications/policy-briefing-data-protection-and-digital-information-no-2-bill-second-reading/

29 Out of sight out of mind? The Prevent referrals that go unrecorded. Prevent Watch (2023) https://www.preventwatch.org/prevent-referrals-unrecorded/#:~:text=Each%20year%2C%20since%202015%2C%20the,over%20the%20last%20eight%20years. Latest Prevent figures: https://www.gov.uk/government/statistics/individuals-referred-to-prevent

30 https://www.legislation.gov.uk/ ukpga/2015/6/schedule/6/enacted

services, social work services, health services, police etc) with whom an individual's data is shared and each of whom has their own policies and processes by which they manage and share the individuals personal information.[31] In some cases, especially where children are involved, the data collection also extends to associated family members, e.g. siblings and parents.

In 2019, FOI requests filed by Liberty revealed that Counter-terrorism had a Prevent Case Management database managed centrally by Counter-terrorism Policing – National Headquarters and is accessible to all police forces across England, Wales, Scotland and Northern Ireland.[32] Despite FOI requests, the Home Office and Counter-terrorism Police have refused to reveal how many individuals are on the Prevent Case Management Tracker – citing exemptions to safeguard national security – which was later discovered to be only one of several police databases that a Prevent referral is stored on.[33]

Much of the Prevent pipeline, and the funnel into the pipeline before an official referral is made, has thus far been unclear, particularly regarding how data is processed and shared. What is known, however, has come under scrutiny by a number of human rights and civil society organisations including Defend Digital Me[34], Children's Rights International Network[35] and Prevent Watch.[36]

Case studies[37] have illuminated that data retention, data sharing and other data rights issues around Prevent are a concern but they have not been systematically addressed. Even the recent (albeit controversial) Independent Review of Prevent published in February 2023[38], conceded that a data retention period of six years for individuals referred to Prevent, when there is no further action taken on their case, should be reduced to three years. However, the recommendation appears arbitrary, without explanation for why three years of data retention in pre-crime standards is any more justified than six years. Often the retention of data extends beyond six years after a review, which may happen regardless of the designated period and enables the indefinite retention of data.

In 2020, in a case brought by Deighton Pierce Glynn, a High Court ruled that the data retention of an 11-year-old child's data was unlawful and disproportionate interference with his right to private life,[39] namely that it was in breach of his Article 8 right under the European Convention on Human Rights, as well as sections 35 and 39 of the Data Protection Act 2018 – that the processing of personal data for any of the law enforcement purposes must be lawful, fair and kept no longer than necessary.

The Prevent referral for this child was made in 2016 and although no counter-terrorism concerns or evidence of radicalisation were found, the Metropolitan Police Service retained the child's data until the judgment in 2020 when the child had reached age 16. They

---

31 See Annex A, a review of policy documents shows a snapshot of the divergence of data sharing policies by different bodies.

32 Grierson, J (2019). Counter-terror police running secret Prevent database. The Guardian https://www.theguardian.com/uk-news/2019/oct/06/counter-terror-police-are-running-secret-prevent-database

33 Grierson, J (2019).Family wins fight to delete child from Met's anti-radicalisation records. The Guardian https://www.theguardian.com/uk-news/2019/dec/19/family-wins-fight-to-delete-child-from-met-prevent-anti-radicalisation-records

34 The State of Data 2020. Defend Digital Me (2020) https://defenddigitalme.org/research/the-state-of-data-2020/

35 CRIN's submission for OHCHR's report on the right to privacy in the digital age. Child Rights International Network (2019) https://www.ohchr.org/sites/default/files/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/CRIN_.pdf

36 Holmwood, J and Aitlhadj, L (2022). The People's Review of Prevent. People's Review of Prevent https://peoplesreviewofprevent.org/main-report/

37 As well as the People's Review of Prevent (ibid) and this report, case studies can be illustrated by the work of Deighton Pierce Glynn E.g. Police Agree to Delete Prevent Referral of Primary School Child (2019) https://dpglaw.co.uk/police-agree-to-delete-prevent-referral-of-primary-school-child/

38 Independent Review of Prevent's report and government response. Gov.uk (2023) https://www.gov.uk/government/publications/independent-review-of-prevents-report-and-government-response

39 Court Finds Data Retention by the Metropolitan Police Service Under the Prevent Strategy Unlawful. Deighton Pierce Glynn (2020) https://dpglaw.co.uk/court-finds-data-retention-by-the-metropolitan-police-service-under-the-prevent-strategy-unlawful/

argued that the retention would have minimal impact on the child but the court ruled that the police service had, "underestimated the impact of the interference with the Claimant's privacy rights entailed in retaining data about his alleged views and statements when he was 11 years old", and went on to conclude that "as long as the Claimant's personal data is retained, he will continue to fear that it may be disclosed to third parties, particularly universities" as there is no guarantee that it would not be disclosed.

It is notable that this significant ruling did not gain any mention in the aforementioned independent review by William Shawcross, which has been widely criticised.

At least two children known to Prevent Watch have had their future education adversely impacted by Prevent referral disclosures despite neither of these referrals progressing to a Channel intervention, making them 'misinformed referrals' by Prevent's own logic.

In one case, 'the case of Tarik' described in the People's Review of Prevent and replicated in **Box 4**, the Prevent referral occurred in the child's early secondary school years and was the reason why a prestigious school withdrew their offer of a sixth form place at the start of the academic year. In the case of Munir (see **Box 5**), the secondary school Prevent referral was used by his sixth-form college to send him home and force him to miss school for over a week without any formal exclusion or disciplinary procedure that his parents could use to challenge the suspension.

BOX 4

CASE OF TARIK

Tarik: Barred from Sixth Form due to Prevent referral, despite achievements.

Tarik was a 16-year-old student due to attend a Sixth Form College known for its higher-than-average proportion of students who go on to prestigious universities.

When Tarik went into the Sixth Form College at the start of the academic year for what he believed would be enrolment, he was surprised to instead find himself being questioned about incidents that had led to a Prevent referral at his secondary school more than two years prior.

The Prevent referral had occurred during his time at secondary school due to a combination of incidents including Tarik correcting his teacher about the definition of jihad and some inappropriate messages in a group chat that led to a fight, for which Tarik had already been sanctioned via a school suspension.

Tarik's parents later found out that Tarik's place had been withdrawn on the basis of "new information" that the Sixth Form College had been given by his secondary school, after the offer had been confirmed.

When asked, the secondary school showed evidence that it had been the Prevent officer who had dealt with Tarik's case and advised the secondary school to ensure that this information was passed on to his Sixth Form once his place had already been confirmed.

Tarik's parent said: "The safeguarding file is supposed to be used to support the child, not to impact decisions of admissions. So, the Sixth Form College has breached something here.

"My child is still a child being only 16 years of age, yet he was questioned about his views on jihad without his parents nor the safeguarding officer present. He was misled to believe this was an enrolment meeting when in fact it was an interrogation of his religious views."

"The impact of this has been huge as it left us scrambling for a new place to send Tarik. It was very strange; how do you then get a clean slate for your child who has done nothing wrong and wants to progress via college, when all the new colleges you apply to will obviously ask why on earth this child has no college, despite it already being September?"

BOX 5

CASE OF MUNIR

Munir: Left in limbo as a result of the smear of Prevent

Munir is a 17-year-old sixth-form student who has previously been referred to Prevent during secondary school. When Munir moved from secondary school to his new sixth form, his safeguarding file containing the information regarding the Prevent referral moved with him.

While in his first year of sixth form studying for his A levels, Munir came to the attention of senior management for breaching uniform policy by wearing his Islamic dress outside of agreed Friday prayer times; Munir was also having doubts about continuing with one of his A level courses that he felt was antithetical to his views as a Muslim. As a result of these two incidents, a senior staff member told Munir to go home as he did not demonstrate inclusive values and mentioned his previous Prevent referral as a reinforcement of this view.

The staff member also told Munir that he should find another school as he clearly did not show the inclusive values required to attend that one. This was not an official suspension or exclusion and Munir's parents did not receive a single piece of paperwork to explain what was happening. Consequently, Munir missed more than a week of school and work for his A levels whilst in limbo.

Munir eventually went back to school but only because of his parents' proactive approach with the school and there was still a failure to document what had happened and why.

This case highlights how Prevent referral information being shared with further educational institutions can harm a child or student, even where no action was taken relating to the original referral.

The earliest point at which personal data is stored is likely the organisation making the referral or through which a report is originally made to show compliance with the Prevent Duty when Ofsted or the Care Quality Commission inspects it. However, the exact details of how these systems work is not clear nor is the extent of record-keeping. For example, do teachers, doctors, safeguarding leads or others record their referrals and in which systems? Due to previous disclosures,[40] we know that once made, referrals are stored within a national Prevent database, regardless of whether they meet the threshold to be reviewed by a Channel panel.

Consent is not necessary for data collation as the data is collected for law enforcement purposes. Consent is only required in response to an offer of an intervention and the referee has the right to refuse.[41] In addition, any public service provider and their staff mentioned in Schedule 6 of the Counter-Terrorism and Security Act 2015[42] would have to process Prevent data.

Disclosures received by ORG, Prevent Watch and Lewis & Klein Associates illuminate a better picture of the Prevent referral process.

40 Liberty uncovers secret Prevent database. Liberty (2019) https://www.libertyhumanrights.org.uk/issue/liberty-uncovers-secret-prevent-database/

41 Channel Duty guidance. Gov.uk (2020) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/964567/6.6271_HO_HMG_Channel_Duty_Guidance_v14_Web.pdf

42 Gov.uk. Schedule 6, Counter-Terrorism and Security Act 2015 https://www.legislation.gov.uk/ukpga/2015/6/schedule/6/enacted

THE REFERRAL PROCESS

The Prevent referral process can be split into four stages:

1. **The initial referral from the provisional identification of a vulnerability risk factor.**
2. **The information gathering of Prevent case officers or counter-terrorism case officers.**
3. **The Channel panel process.**
4. **The individual's exit from Channel.**

STAGE 1: REFERRAL FROM EDUCATION, HEALTH OR OTHER SCHEDULE 6 INSTITUTIONS

Prevent referrals are generally fed by individual staff to a senior manager or designated safeguarding lead. A conversation may take place over the phone with the police Prevent contact. In general, the local inter-agency procedure would be followed or a Prevent referral form would be completed[43] and sent to the Prevent team of the regional police force, which may include the following information about the individual.[44]

- **Full names (including aliases and spelling variations)**
- **Date of birth**
- **Genders of children in the household**
- **Family address**
- **School/nursery (if relevant)**
- **Parents/guardians plus other main caregivers**
- **Names and date of birth of all household members**
- **NHS number**
- **Education unique pupil number (if relevant)**
- **Ethnicity, first language and religion of children and parents**
- **Any special needs of children or parents**
- **Any significant/important recent or historical events/incidents in the child or family's life**
- **The cause for concern, including details of any allegations, their sources, timing and location**
- **Child's current location and emotional and physical condition**
- **Whether the child needs immediate protection**
- **Details of the alleged perpetrator (if relevant)**
- **Referrer's relationship and knowledge of child and parents**
- **Known involvement of other agencies/practitioners (e.g. GP)**
- **Information and parental knowledge of/agreement to the referral**
- **The child's views and wishes (if known)**

The form collects both personal and special category data.

Referrals can also be added to the Prevent system informally. If a member of the public or partner institution contacts a counter-terrorism case officer seeking advice, the case officer may also choose to submit that case as a referral to Prevent should they think it necessary. The person seeking advice would be informed of this.

The exact data collected differs between each local authority and the police do not have the power to mandate specific data collection practices.

43 Prevent. Southampton City Council https://www.southampton.gov.uk/council-democracy/partnership-working/safe-city/prevent

44 An example taken from Referrals process, Halton – Children and Young People Safeguarding Partnership Online Procedures

FIGURE 1

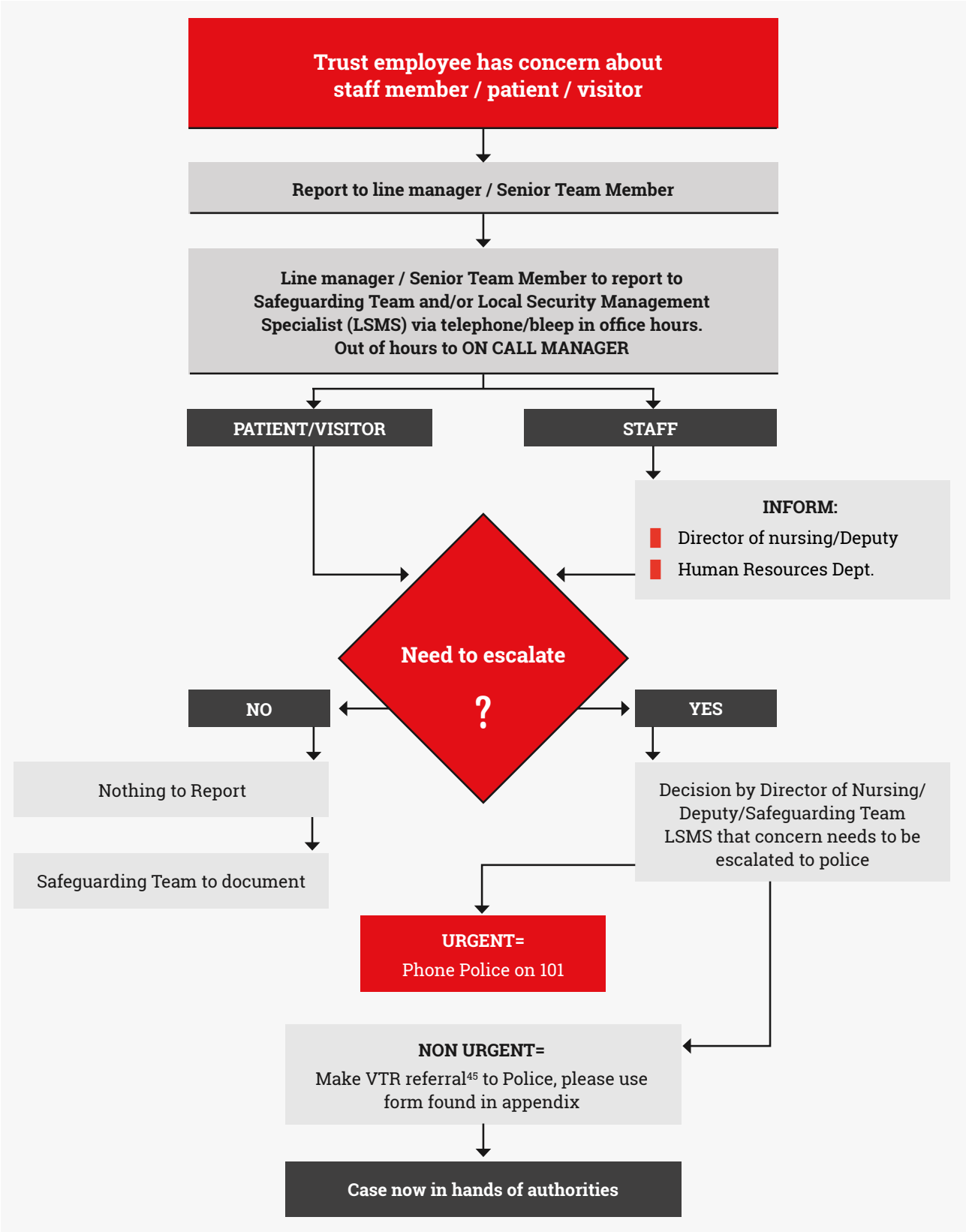


Figure 1 Example referral process within the referring institution.[46]

45 VTR refers to 'Vulnerable to Radicalisation'.

46 James Paget University Hospitals Prevent Policy (Annex A).

STAGE 2: PREVENT REFERRAL ONCE IT IS SENT TO THE POLICE PREVENT TEAM[47]

Prevent case management and local records

In all instances after a referral has been received the referral is logged immediately on the Prevent Case Management Tracker.

While advice not resulting in a referral is omitted from entry onto the Prevent Case Management Tracker, it is considered good practice to retain a record on local systems or within a pocketbook.

Where necessary, additional biographical data may be drawn from local police systems to complete any missing data.

Recording shared information

A standardized template for information sharing between the police and local authorities indicates that where information is shared from police systems, a record will be made of this share within those systems.

A record of the personal information disclosed to a partner agency will be created on CRIMINT PLUS by the disclosing officer at the time the information is supplied (or as soon as possible thereafter) unless this disclosure record has already been made on another police system (e.g. ViSOR, MERLIN or CRIS).[48]

Deconfliction and Pursue checks

Before any Prevent activity begins, a deconfliction process is undertaken – deconfliction is the process of determining when law enforcement are concurrently conducting an event in proximity.
The counter-terrorism case officer checks with local Fixed Intelligence Management Units whether any intelligence held indicates that the referral should be moved to the Pursue space – another tranche of the government's CONTEST strategy to detect and understand, investigate and disrupt terrorist activity in the UK or against UK interests.[49]

This process should take no more than five working days and includes checks across the following databases at a minimum:

- **Secure CT Intel system**
- **Local Intelligence & Crime Systems**
- **Police National Computer**
- **Police National Database**
- **CTHolmes**

Where there is no indication of Pursue relevance, the Prevent team will be informed and any research documents shared. Prevent-related activity can then begin.

Police gateway assessment

A police gateway assessment will be used to assess the risk of the referee, using a tool called the Dynamic Investigation Framework.[50] This assessment should be completed within five working days. Completing the dynamic investigation framework involves drawing data from the following databases, if the information was not made available from the Fixed Intelligence Management Unit:

- **Police National Computer**
- **Police National Database**
- **NCIA (National Common Intelligence Application)**
- **Open Source**
- **Local Crime & Intel Systems**
- **CTHolmes (where available)**

---

47 Counter-Terrorism Policing HQ - Prevent Case Management by CTCOs & CTCO Supervisors (August 2020). (Annex A)

48 Data Sharing Agreement (DSA) For the Channel Panel Between MPS and London Borough of Tower Hamlets, 2020, p.10. (Annex A)

49 CONTEST: The United Kingdom's Strategy for Countering Terrorism. Gov.uk (2023) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1186413/CONTEST_2023_English_updated.pdf

50 No further details were attained of this tool.

Contact during police gateway assessment

In most instances, partner agencies will not be contacted as part of the police gateway assessment. Visiting the referee during the gateway assessment is also not recommended or necessary.

However, if a pressing safeguarding issue or other immediate concern presents itself during the police gateway assessment, a visit can be undertaken by a counter-terrorism case officer, another safeguarding official, or both. If such a visit is carried out, consent for Channel should not be sought at this stage.

If the referee raises the issue themselves, any decisions should still be deferred until a decision (made under section 36 of the Counter Terrorism and Security Act 2015) has been made for a Channel referral.[51]

In the case of foreign nationals

If the subject is a foreign national, then consideration must be given to contacting the Foreign, Commonwealth and Development Office, the Criminal Records Office and Immigration Services to identify whether the subject has any convictions abroad or whether other intelligence about activities outside the UK is held.[52]

Information gathering

If during the police gateway assessment phase, a reasonable suspicion of a Prevent-relevant concern is found, the case is kept in the Prevent Case Management Tracker and the case will move to the "information gathering phase".

In areas participating in the Dovetail pilot – a trial transferring resources and responsibilities for administering and case managing Channel from the police to local authorities – the information gathering phase is undertaken by the Local Authority Channel Coordinator.

Throughout the police gateway assessment and information gathering phase processes, Fixed Intelligence Management Units will be updated with any new intelligence on the referee. Summaries should be shared at least every three months, or when perceived escalations in risk have occurred. This includes up-to-date biographical data and data on known associates.

Additionally, referees who are juveniles or who show a propensity to travel to conflict zones should be considered for inclusion on a Ports Intelligence Watchlist.

Section 36 decision

After the case management and information gathering phases are complete, a section 36 decision (see above) will be made as to whether the subject should be referred to a Channel panel to discuss interventions.

If a reasonable belief that there are no Prevent or Pursue relevant concerns with the case, it will be closed at this phase. The data will be retained according to the Management of Police Information (MOPI) guidance[53].

Following a section 36 decision, the case is entered into the Channel Management Information System,[54] a web-based case management system controlled by the Home Office[55] – except where there is an escalation of counter-terrorism risk, the police cannot remove a case from Channel once it has been accepted without the agreement of the Channel panel.

---

51 Section 36 of the Counter-terrorism and Security Act 2015 places a statutory duty on local authorities to convene Channel panels to assess individual referrals. A decision to intervene is known as a section 36 decision.

52 Counter-Terrorism Policing HQ - Prevent Case Management by CTCOs & CTCO Supervisors (August 2020) (Annex A)

53 College of Policing. Management of police information https://www.college.police.uk/app/information-management/management-police-information

54 CTP-HQ are planning to merge the Prevent Case Management Tracker and CMIS databases in the future.

55 User Guide to: Individuals Referred to and Supported through the Prevent Programme, England and Wales. Home Office (2023) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1186413/CONTEST_2023_English_updated.pdf

STAGE 3: INTERVENTIONS VIA CHANNEL OR POLICE-LED PROCESS

Suitability for Channel

Following a section 36 decision, a multi-agency Channel process could be initiated if the threshold is met.

As stated in the government's Channel Duty Guidance,[56] the Channel panel assesses vulnerability using the Vulnerability Assessment Framework built around three dimensions:

- **Engagement with a group, cause or ideology**
- **Intent to cause harm**
- **Capability to cause harm**

Interventions could include:

- **Life skills**
- **Mentoring/one-to-one support, including with an intervention provider**
- **Anger management programmes**
- **Cognitive/behavioural therapies**
- **Constructive pursuits e.g. sport or arts**
- **Employment, education and training support**
- **Family support e.g. formal parenting programmes**
- **Health checks, including physical and mental health**
- **Housing/tenancy services**
- **Drugs and alcohol misuse interventions**

The Channel coordinator and Channel coordinator supervisor will discuss cases that meet the threshold for possible referral to the Channel programme at a monthly Channel panel.

Channel is local authority-led but counter-terrorism case officers will still be involved in the channel process, attend all Channel panels and fulfil the police role as a statutory partner – counter-terrorism subject matter expert – disclosing police-held intelligence necessary for decision-making.

Non-Prevent police may also be invited by the Channel chair. Police involvement stretches to risk assessing deployment of intervention providers[57] to a subject and risk escalation with a potential Intelligence Handling Management leader Priority Operation and referred to the Fixed Intelligence Management Unit for urgent assessment.

If a case is not suitable for Channel then the Channel supervisor will inform the police Prevent supervisor of the decision so that any pertinent actions can be followed up by them i.e. additional checks based on any new information gathered. If another type of referral system is underway, that may be deemed sufficient.

Any Channel panel will have a chair and could include representatives from any of:[58]

- **Children and Adult Social Care**
- **Health Sector**
- **Youth Offending**
- **Counter-Terrorism Unit**
- **Prisons**
- **Early Help Services**
- **Safer City and Communities**
- **Probation**

56 Gov.uk (2023). Channel duty guidance: Protecting people susceptible to radicalisation https://assets.publishing.service.gov.uk/media/651e71d9e4e658001459d997/14.320_HO_Channel_Duty_Guidance_v3_Final_Web.pdf

57 Ideological and theological specialists are considered to have the tools to counter extremist narratives.

58 Stoke-on-Trent Prevent Referrals and Channel Process (Annex A); Derbyshire child safeguarding partnership agreement (Annex A); City of London Prevent Policy (Annex A).

- **Voluntary organisations**
- **Other appropriate service as deemed necessary by the case**

Any disclosure of personal information is recorded on CRIMINT PLUS.

The Channel Full Assessment Tool and Channel Guidance as issued by the Home Office is used to guide decisions about whether an individual needs an intervention to address their vulnerability to radicalisation.[59]

The type of information that could be shared includes:

- **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 inside 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 provided by family/carers and/or other organisations (e.g. GP, school nurse, police)**
- **Reports relating to the 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**
- **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)**
- **Racial or ethnic origin**
- **Political opinions**
- **Religious or philosophical beliefs**
- **Data concerning health**
- **Sex life/sexual orientation**

Police-led partnership process

Where cases have a Prevent concern but are inappropriate for Channel, the police can instead manage the case within a police-led partnership. This process is police-led in partnership with non-police agencies and non-Prevent policing. Cases dealt with by a police-led partnership are deemed unsuitable for Channel but nonetheless are still deemed Prevent-relevant due to ideological or risk factors. Police-led partnership cases can involve individuals or cases where no individual has been identified, such as with racist stickering locally.

Typically, police-led partnership cases are not suitable for Channel because the referee might be a family member of a subject of interest or they have refused Channel support.

59 Channel duty guidance: protecting people susceptible to radicalisation https://www.gov.uk/government/publications/channel-and-prevent-multi-agency-panel-pmap-guidance/channel-duty-guidance-protecting-people-susceptible-to-radicalisation-accessible

Alongside safeguarding activities similar to Channel, police-led partnership cases can also be subject to disruptive measures, and a wider range of agencies can be present at a police-led partnership panel to assist.

Such partners can include:

- **Social Services**
- **UK Border Agency**
- **Environment Agency**
- **DVLA**
- **National Crime Agency**
- **Trading Standards**
- **HMRC**
- **Fundraising Standards Commission**
- **Intelligence Services**

The police-led partnership chair will decide and explain, on a case-by-case basis, who should be present at a police-led partnership panel and in what circumstances, and this must be recorded along with a rationale on the Prevent Case Management Tracker.

The wider array of partners support disruptive activities, which can include:

- **Investigating and prosecuting any anti-social behaviour and offences by Prevent subjects, not just terrorism offending.**
- **Compiling evidence and building files to support the local authority in taking safeguarding action, up to and including Wards of Court procedures.**
- **Supporting counter-terrorism case officers to explore opportunities to investigate and prosecute individuals of interest for non-Terrorism Act offences to undermine their status or credibility and limit their activity.**

STAGE 4: OUTCOMES, CASE CLOSURE AND CASE TRANSFER

Cases that have been entered into the Prevent Case Management Tracker can be closed in five ways:

- **Subject deceased**
- **Judged to have no counter-terrorism concern**
- **Subject unlocatable**
- **Case escalated to Pursue**
- **No counter-terrorism concern and case referred elsewhere**

If a case reaches the police gateway assessment, then the dynamic investigation framework must also be completed before closure. Cases diverted to a police-led partnership process can be closed when the subject is thought to be successfully deterred, diverted or desisted. However, a decision can also be made to close a police-led partnership case if there is a low-level counter-terrorism risk. The case can also be monitored before closure.

Cases that have reached a Channel panel can be closed where the panel considers all counter-terrorism and safeguarding concerns to be addressed or where they are convinced that the subject is receiving adequate support elsewhere. A vulnerability assessment framework should be carried out before closure to monitor risk. At six and 12 months, the case should be reviewed. Once the 12-month review is complete, a referee is considered to no longer be on the Channel programme. The data is reviewed six years after this point.

FIGURE 2

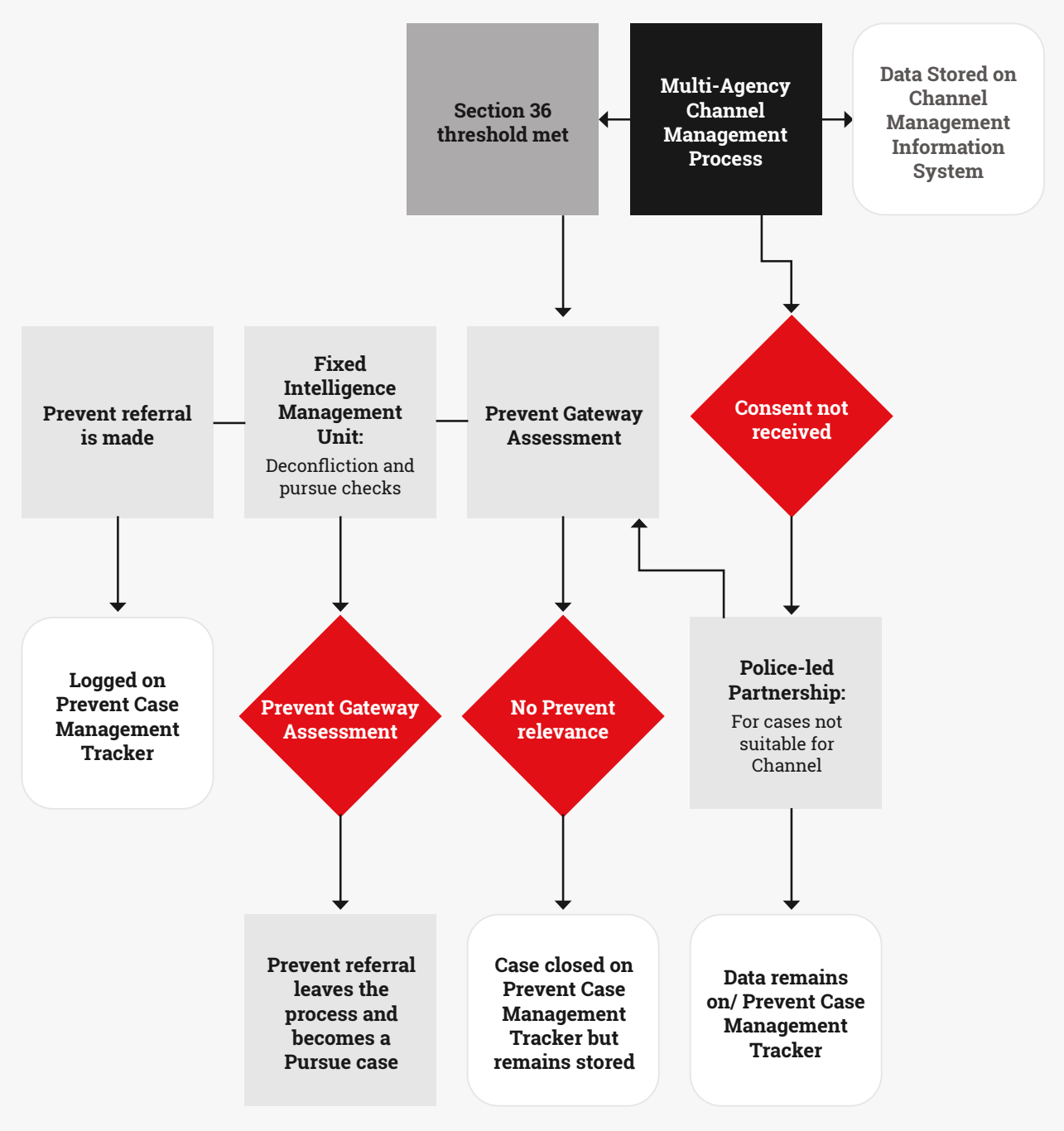


Figure 2 The Counter-terrorism Policing Prevent referral process as interpreted from the Prevent Case Management Guidance[60]. Source: Charlotte Heath-Kelly, Professor of Politics and International Studies at University of Warwick

60 Counter-Terrorism Policing HQ (2020). Prevent Case Management Guidance. (Annex A)

FIGURE 3

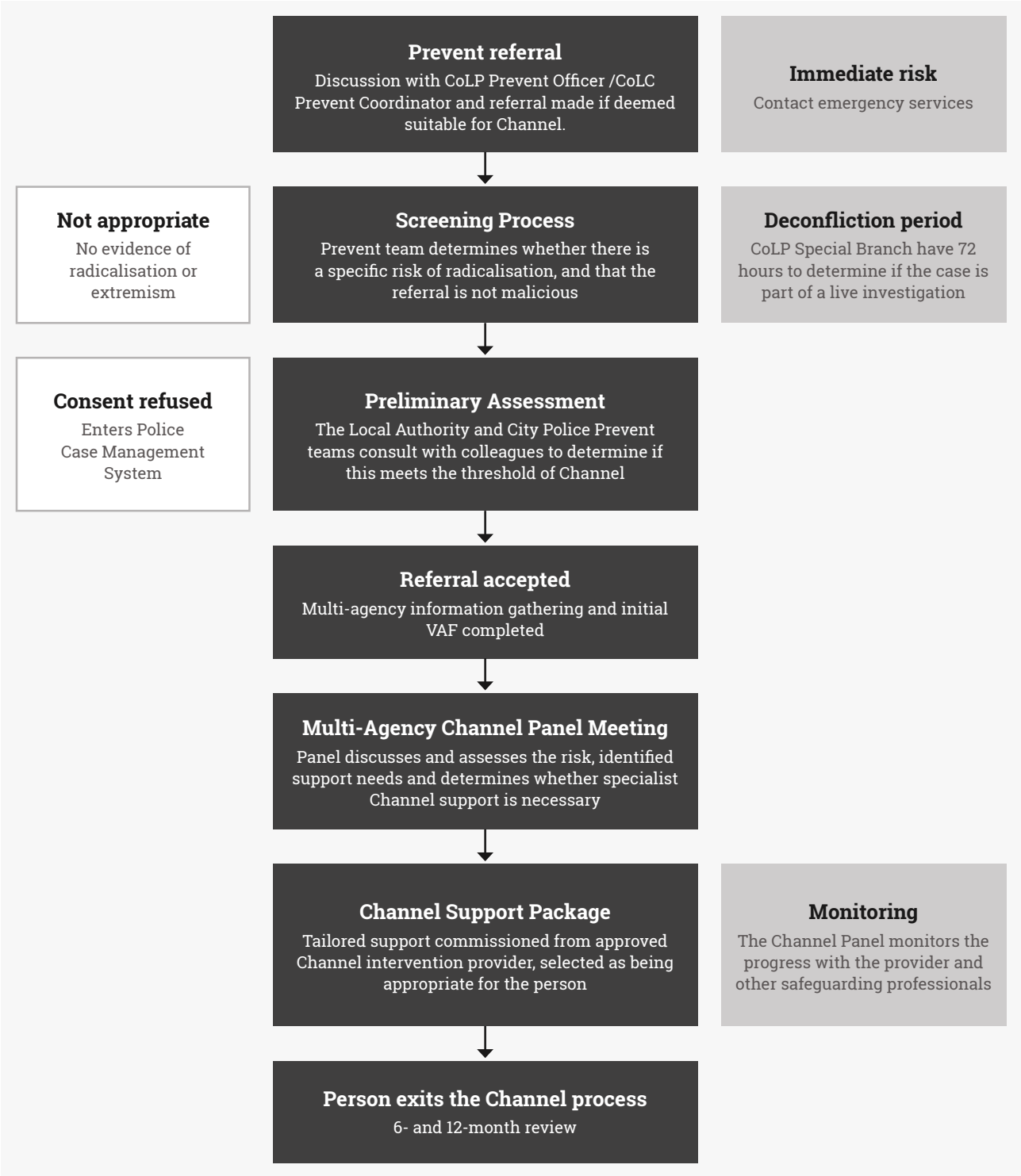


Figure 3 Prevent referral flowchart demonstrated by the City of London. Source: City of London Prevent Policy[61]

The above chart demonstrates the different stages an individual's data passes through if they are referred under Prevent.

61 City of London (2021). City of London Prevent Policy and Guidance (Annex A)

BOX 6

KNOWN DATABASES HOLDING PREVENT DATA[62]

- **Prevent Case Management Tracker (PCMT)**
- **London Prevent Case Management Excel spreadsheet – accessible to MPS Counter-terrorism Officers**
- **Merlin Report**
- **CRIMINT**
- **CRIMINT PLUS**
- **DevPlan**
- **MPS's Computer Aided Despatch System**
- **Prevent Case Management Tracker application**
- **National Master Prevent Case Excel spreadsheet**
- **National Counter-terrorism Policing Headquarters system (NCIA/NSBIS)**
- **Channel Management Intelligence System (CMIS)**
- **STOPS**
- **Central Registration and Identification System (CRIS)**
- **Police National Computer**
- **Police National Database**
- **Computer Aided Dispatch (CAD)**
- **Ports Intelligence Watchlist (PIW)**

62 Liberty uncovers secret Prevent database (2019). Liberty https://www.libertyhumanrights.org.uk/issue/liberty-uncovers-secret-prevent-database/; Prevent Case Management Guidance. (Annex A); The Queen on the application of II (by his mother and Litigation Friend, NK) - and - Commissioner of Police of the Metropolis [2020] EWHC 2528 (Admin). DPG Law https://dpglaw.co.uk/wp-content/uploads/2020/09/2951202-R-II-v-Commissioner-of-Police-of-Metropolis-2020-EWHC-2528-Admin-final-judgment.pdf

PROTOCOLS FOR DATA RETENTION AND STORAGE

As highlighted in the section above, information could be sought from various agencies and institutions to feed into an individual Prevent referral. Any subsequent Channel panel will involve information sharing between numerous bodies if applicable. There is often the same guidance around data processing for a Channel panel. However, for a Prevent referral, data retention and storage protocols can differ significantly in each case.

For example, even where a Prevent referral does not result in a Channel intervention and is classed as a misinformed referral even by Prevent's own logic, the data is held on police databases for at least six years – following the initial six and 12-month reviews with the vulnerability assessment framework. After this additional six-year period, another review is conducted to assess if referral data should be held for another six years.[63]

The individual concerned is not informed that their data is being stored nor whether their data has been deleted after the six-year period or further retained. Also of significance is the storage of data on children's services records at the local authority of a child referred.[64] Even if they have not been previously known to social services, a Prevent referral is shared with children's services and this information is kept for 25 years after the child's 18th birthday.[65] It would therefore still be available when that child is an adult and has children of their own, thus impacting any future assessment concerning their own children and any children's services interventions.

BOX 7

NATIONAL RETENTION ASSESSMENT CRITERIA

According to MOPI section 7.4, which governs the retention of personal data provided via a Prevent referral:

All records which are accurate, adequate, up to date and necessary for policing purposes will be held for a minimum of six years from the date of creation. This six-year minimum helps to ensure that forces have sufficient information to identify offending patterns over time, and helps guard against individuals' efforts to avoid detection for lengthy periods.

Beyond the six-year period, there is a requirement to review whether it is still necessary to keep the record for a policing purpose. The review process specifies that forces may retain records only for as long as they are necessary.

In addition to data processed by police and local authorities, those who have made the original referral will have their own mechanisms for recording concerns that may or may not have led to a Prevent referral and these record systems and potential data sharing agreements between institutions will vary.

63 Guidance on the Management of Police Information MOPI, Second Edition, section 7.5

64 Tower Hamlets (2020). Purpose Specific Data Sharing Agreement (DSA) For the Channel Panel Between MPS and London Borough of Tower Hamlets. (Annex A)

65 Blackburn with Darwen Council Privacy Notice for Community Safety – Prevent (Annex A).

BOX 8

THE CASE OF NOAH

Noah: Denied access to how personal data was processed

A 14-year-old non-Muslim was referred to Prevent in 2018 because of concerns raised by another pupil about his social media content. According to his referral, he demonstrated a fascination with the Middle East and militarism. At the same time, his views on Israel were sympathetic to its Jewish population and he had spoken to a Rabbi about converting to Judaism – professionals put it down to child curiosity rather than radicalisation and that the state intervention – via a Prevent referral and subsequent section 17 or 'child in need' assessment under the Children Act 1989 was likely to have had a negative impact on him. The Prevent referral said he was vulnerable to far-right and Islamist extremism but the family rejected a Channel referral.

They also submitted a SAR for the boy's information to the local authority, which it refused to disclose. The ICO concurred with the local authority's decision not to release the letter as it contained third-party data. The school conceded by disclosing a heavily redacted version of the original referral letter.

The family then learned the boy's Prevent referral data would not be deleted because MOPI guidelines dictated a minimum retention period for review (six and 12 months) and that unless he had any brushes with the law it would be deleted.

The boy was then subject to a second Prevent and Channel referral in 2019 because he had allegedly visited a far-right chatroom. He said he was invited to the WhatsApp group through a link and was asked to answer five screening questions, his answers failed their admission requirements and he was removed from the chat immediately.

His details came to the police's attention when members of the far-right group were arrested and his number was found associated with the WhatsApp chat. Police were concerned he was vulnerable to being groomed. The incident was used to double down on the insistence that the original referral was justified. Following further state intervention, the Prevent referral was not deemed beneficial but it took five months before the discharge letter from the Channel panel was received, which was needed to close the case on the national Prevent database.

The family submitted another SAR to the council, which released more information with the exemption that "personal data processed for the purposes of safeguarding national security or defence is outside the GDPR's scope and therefore is not eligible for release under Subject Access."

SARs to the police revealed that the boy's details would be held in accordance with the national assessment criteria but noted that it was linked to data concerning terrorism, which would put the review period at 10 years. The police were unable to list which agencies the data had been shared with.

POLICE PROCESSING OF PERSONAL DATA

What's recorded?

As shown above, all Prevent referrals are recorded on the national Prevent Case Management Tracker but they may arrive through a variety of avenues. Responses to FOI requests show that the Counter-terrorism Policing Prevent team are promoting the use of a universal referral form[66] to standardise data entry, although this is not mandated and in some cases, other referral forms are used and may be inappropriate to replace. Information may also be phoned in and not use an official paper-based referral at all.[67]

Phone-ins may also be for advice, however, and the guidance states that calls for advice should not be logged onto the Prevent Case Management Tracker. The guidance recommends phone-ins are recorded on local systems and in pocketbooks.[68]

How is the information managed?

There are currently no Prevent-specific guidelines for the processing of personal information. Instead, Counter-terrorism Policing applied the widely used framework of MOPI,[69] available on the College of Policing website.[70]

As stated in the MOPI guidance, for data to be legally held by police there must be a policing purpose, which can include preventing an offence from happening, as defined in law. If Prevent is the deterrent to terrorism, then terrorism could be the offence being prevented for the purposes of managing police information and thus subject to the highest thresholds for retention.

Right to privacy

All policing information against an individual is considered personal data and is thus governed by the eight data protection principles mentioned under the section covering 'The UK Legal Framework for Data Protection'.

Therefore, even though law enforcement exemptions apply, they can only be applied case-by-case and there is no catch-all exemption for police use of data. Section 29 of the Data Protection Act 2018 may also apply, stipulating an exemption on national security grounds.

Moreover, the need to hold data for policing purposes must be balanced against the right to privacy as enshrined in the Human Rights Act 1998 and data protection legislation. Therefore, officers must apply a proportionality test to determine if the need to hold the data warrants any infringement of the right to privacy. The more intrusive the data, the higher the threshold this proportionality test must meet.

Mitigating data risks

According to UK GDPR, anyone processing personal data likely to result in a high risk to individuals must conduct a DPIA. The DPIA helps identify and mitigate the risks of processing personal data including infringements of human rights. Organisations processing personal data are encouraged to complete a screening checklist to help decide if a DPIA is necessary. A high risk would be determined from a "high probability of some harm, or a lower possibility of serious harm."

Ultimate accountability in law for the management and processing of the data lies with the data controller, which in the case of policing information is the Chief Police Officer.

---

66 Counter-Terrorism Policing HQ - Prevent Case Management by CTCOs & CTCO Supervisors (August 2020) (Annex A).

67 Ibid.

68 Associated Professional Practice – Management of Police Information – Review, retention and disposal. College of Policing (2023) https://www.college.police.uk/app/information-management/management-police-information/retention-review-and-disposal

69 The Counter-Terrorism Policing Prevent referral process – Authorised Professional Practice. College of Policing (2013) https://www.college.police.uk/app/information-management/management-police-information

70 Management of police information. College of Policing https://www.college.police.uk/app/information-management/management-police-information

In the case of Prevent, one DPIA exists covering both the Prevent Case Management Tracker and Channel Management Information System. Where there is a police-led process for Prevent, the Prevent Case Management Guidance states that it is unnecessary to undertake a separate DPIA for each process for every region or force.[71]

Retention periods

As noted in the MOPI guidance, the National Retention Assessment Criteria apply to any type of retention of policing information. This criteria is applied to Prevent Case Management Tracker entries.

According to the MOPI guidance, any entry that satisfies the criteria necessary for policing purposes should be kept for a minimum of six years[72] after its six and 12-month review – if it doesn't satisfy the criteria then it should be deleted. The rationale for this minimum retention period is to consider the possibility of "re-offending". However, an initial offence would not have been committed under Prevent. Therefore, this rationale to retain data is not fit for purpose.

Retention and review periods – to assess if retention periods need extending – are tied to another assessment around the "offending" behaviour. That includes the risk of inflicting serious harm, whether there has been a serious breach of trust, concerns about substance misuse and whether an individual's mental state could exacerbate risk.

Retention periods are also tied to the 'type' of policing purpose, according to the following groups:

Group 1 - Certain Public Protection Matters – including "potentially dangerous people" – until age 100. A review must take place every 10 years. As Prevent sits within the government's counter-terrorism strategy, data retention could be justified for up to 100 years.

Group 2 - Other Sexual, Violent or Serious Offences as defined by the Police National Legal Database. Retained only as long as they are considered a risk of harm but for 10 years minimum; if there is continued offending, then the data can be retained outside of normal schedules, known as a 'triggered' review.

Group 3 - All other offences defined in the force's information management strategy, which mandates the minimum retention period (six years following a six and 12-month review).

Case closure and disposal

Every Prevent referral entered on the Prevent Case Management Tracker will eventually require a closure 'outcome' as the referral moves through the relevant referral process. Every entry is referred to as a 'nominal' and is given one of the following status designations on the system: 'no further action,' 'arrested', 'acquitted' or 'charged.'

According to MOPI guidance, "nominals" recorded as 'group 3' can be manually deleted without review. However, in such cases, mechanisms need to be in place to identify records that should be excluded from that process, particularly those relevant to any activity that could be seen as a precursor to more serious offending. The guidance also states that data quality is sufficient for automated decision-making. For groups 1 and 2, the guidance suggests that the risk of serious offences means that "consideration must be given to the national record and the review must include a [Police National Computer] and [Police National Database] check."

Disposal of records is set and conducted under the information management strategy and Association of Police Officers Information Systems Security Policy and must occur when a policing purpose no longer exists, which will likely be determined after a review. There appear to be no safeguards for the disposal of records, particularly of children referred to Prevent whose information is then kept on police databases those suspected or convicted of crimes as demonstrated by the case of Sami in **Box 9.**

71 Counter-Terrorism Policing HQ - Prevent Case Management by CTCOs & CTCO Supervisors (August 2020) (Annex A).

72 The six year period commences after the 12 month review, so the total period is seven years.

BOX 9

CASE OF SAMI

Sami is a six-year-old boy who was referred to Prevent when his father refused to engage with Prevent officers.

Sami's details were held on police databases and when his parents asked for the data to be removed the police justified retaining his personal details with the following explanation:

"Police are obliged to retain records of calls for service for a policing purpose which includes the prevention, investigation, detection or prosecution of criminal penalties; safeguarding against and the prevention of threats to public security."

However, this data deletion request was for the six-year-old who was not involved in any crime, and in fact neither was his father. After the father pursued the matter further and challenged the refusal to remove the child's data, the police finally responded by saying that they would remove the data but that other police forces may have the data and it would be for the parent to ask those individually for its removal.

LOCAL AUTHORITY DATA PROCESSING FOR PREVENT

How is the information managed?

Local authority partners are to be considered joint data controllers for the processing of data, particularly for Channel panels, therefore, they should have a DPIA in place.[73]

While MOPI provides a framework for Counter-terrorism Policing and other police forces' handling of Prevent data, there is less guidance for local authorities around consistent data handling. Each local authority operates according to its own Prevent and privacy policies or those of the regional hub to which it belongs. Therefore, there is no overarching guidance for how Prevent data is retained and stored except that it must be done in compliance with data protection and human rights legislation. Some authorities point to the Home Office's general privacy policy covering the Channel process.

Retention periods

There is evidence that local authorities have their own retention period guidelines and systems on which data is recorded.[74] Even if specific data from Prevent referrals is removed following Home Office guidelines about the Channel process, numerous referrals of children never progress to Channel but are flagged with children's services and, therefore, result in data being stored about entire families.

This data retention appears unnecessary as the typical eventual outcome from social services is a decision that 'no further action' is required following an assessment. Nevertheless, personal information and intimate family details will remain on the

73 Purpose Specific Data Sharing Agreement (DSA) For the Channel Panel Between MPS and London Borough of Tower Hamlets (Annex A).

74 For instance in the Purpose Specific Data Sharing Agreement (DSA) For the Channel Panel Between MPS and London Borough of Tower Hamlets (Annex A), it states that other information held on partner networks will be managed and deleted in accordance with the corporate information management policies of the organisation; a data sharing agreement between Counter-terrorism Policing South East [and others] states that the information will be held in line with the respective organisation's retention period; Data Sharing Agreement between Counter-terrorism Policing South East [and others] (Annex A).

system for 25 years after the child reaches 18 years of age, simply because they were referred to and assessed by children's services. This could be the case for the thousands of child Prevent referrals that occur each year.[75]

Privacy notice

Of the tens of local authorities we received responses from, only Blackburn with Darwen used a clear and detailed form that Prevent referees would receive when assenting to a Channel intervention. All other areas used some form of generic privacy notice, available online, which outlined in varying detail the data collected, where it was stored, shared and how long it would be retained for. Tower Hamlets indicated that it did not have any such specific information.

Reviewing the various privacy notices, there was inconsistent and generally inaccurate information available to participants. Some information available was too complex to be deemed appropriate, especially for vulnerable persons or children. Under the Data Protection Act 2018, if consent is the lawful basis for processing, individuals should be made aware of how their data is used.

Safeguarding

Prevent referrals – particularly when children are subject to them – can be subsumed within other safeguarding processes. Safeguarding processes and protocols could have their own set of forms, databases, recording standards and retention periods that may or may not align when Prevent referrals are made outside of safeguarding.

For example, the Barking & Dagenham, Havering and Redbridge Child Safeguarding Handbook[76] states that child protection conference reports will potentially be scanned into all children's folders in compliance with NHS codes of practices regarding records management. Full minutes may be scanned in where children are concerned whereas only a summary is required for adults. It is unclear if these records could become 'health data' subject to further processing.

PREVENT WITHIN THE NHS

How is the information managed?

Between March 2021 and 2022, 11% of all Prevent referrals came from the health sector.[77] However, Prevent guidance to support healthcare workers in the local delivery of Prevent has existed since 2011. Prior to the introduction of the Prevent Duty, guidance tapped into already existing safeguarding arrangements, noting that 'every healthcare organisation will have in place existing arrangements for reporting concerns which comply with good governance and safeguarding practices'.[78]

Guidance post-2015 does not drastically re-frame guidance around Prevent for healthcare workers. Rather, it confirms that the Prevent Duty sits alongside existing safeguarding arrangements.[79]

---

75 Blackburn with Darwen Council Privacy Notice for Community Safety – Prevent (Annex A).

76 Barking & Dagenham, Havering and Redbridge Child Safeguarding Handbook

77 Official Statistics Individuals Referred to and Supported through the Prevent Programme, April 2021 to March 2022. Home Office (2023) https://www.gov.uk/government/statistics/individuals-referred-to-and-supported-through-the-prevent-programme-april-2021-to-march-2022/individuals-referred-to-and-supported-through-the-prevent-programme-april-2021-to-march-2022#people-referred-to-the-prevent-programme

78 Building Partnerships, Staying Safe The Health Sector Contribution to HM Government's Prevent Strategy: Guidance for Healthcare Workers. Department of Health and Home Office (2011) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/215253/dh_131912.pdf

79 Guidance: Prevent and the Channel Process in the NHS: Information Sharing and Governance. Department of Health and Social Care (2022) https://www.gov.uk/government/publications/prevent-and-the-channel-process-in-the-nhs-information-sharing-and-governance/prevent-and-the-channel-process-in-the-nhs-information-sharing-and-governance#necessary-proportionate-and-lawful-to-share-information

Safeguarding

The NHS guidance draws on the ICO guidance and the data regime set out above applies, safeguarding and the Prevent work sitting within this framework. For example, the Primary Care Safeguarding Handbook lists Prevent as only one of many safeguarding issues. There is no supplementary context around data processing imposed as part of the Prevent Duty but there is a reference to and recitation of national guidelines.[80]

The handbook also points practitioners to the national NHS Safeguarding Guide app which supports health workers and contains a section on Prevent, again framed in the wider context of safeguarding.[81] As with all safeguarding concerns, 'timely and effective information sharing is a key element of Prevent'. The documentation emphasises that having clear organisational policies and procedures in place is key to ensuring data security and that any data sharing must sit within the GDPR and Data Protection Act 2018 legal framework.[82]

Data processing guidelines

This guidance also highlights that when information sharing agreements are put in place, they should refer to Prevent to facilitate seamless data sharing between relevant partners.[83] Guidance issued to the James Paget University Hospitals explicitly states that:

Measures should be put in place so vulnerable people are supported and protected whilst receiving NHS care from any risk of radicalisation. Health staff already have a duty to report concerns about abuse or exploitation of vulnerable adults. Raising concerns through Prevent will be no different.[84]

The same document also notes that the trust will not take on surveillance or enforcement activities under Prevent.[85] Conversely, the North Cumbria Integrated Care NHS Foundation Trust does not follow this guidance, stating that 'the trust does not hold any data sharing agreements, data protection impact assessments or data processing contracts specifically for either Prevent or Channel'.[86]

The Department of Health and Social Care guidance sets out in detail what NHS trusts and clinical commissioning groups must do to ensure that all data sharing complies with the current GDPR and Data Protection Act 2018 rules and regulations. This guidance does not reference how long any Prevent-related data should be retained. NHS Digital provides some guidance to the public on how to delete personal data. However, whether this includes Prevent-related data is not clear.[87]

---

80 Guide to the UK General Data Protection Regulation (UK GDPR). ICO (2023) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr; FOI response Barking and Dagenham, Havering and Redbridge, NHS North East London (Annex A).

81 NHS England Safeguarding App. NHS England (2023) https://www.england.nhs.uk/safeguarding/nhs-england-safeguarding-app

82 NHS England (2017). Practical Guidance on the Sharing of Information and Information Governance for All NHS Organisations Specifically for Prevent and the Channel Process https://www.england.nhs.uk/wp-content/uploads/2017/09/information-sharing-information-governance-prevent.pdf

83 Practical Guidance on the Sharing of Information and Information Governance for All NHS Organisations Specifically for Prevent and the Channel Process (Annex A).

84 James Paget University Hospitals Prevent Policy (Annex A).

85 Ibid.

86 North Cumbria Integrated Care Trust (2023). FOI response to Prevent questions from Uni of Lincoln researchers (Annex A).

87 Retention and Disposal - Personal Data Consideration. NHS Digital (2022) https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/records-and-document-management-policy/retention-and-disposal---personal-data-considerations

Special category data

GDPR and Data Protection Act 2018 rules outline the following special circumstances in which healthcare operators are allowed to retain special category data:

a) if the data is necessary for public health interest – which is rather broadly defined

b) if the data is necessary for the purpose of preventative or occupational medicine

Prevent is not mentioned as an exemption, so the assumption is that data will be deleted after the required period of time and in line with the Health and Social Care data provisions outlined in Appendix II. The date for this will depend on how the data has been categorised.

Data storage

The North Cumbria Integrated Care NHS Foundation Trust states that the data collected under Prevent is stored in accordance with NHS England guidelines.

Staff must report concerns to the senior team leader who will raise the referral with the respective Safeguarding team, or in cases relating to staff, Human Resources, as well as the Caldicott Guardian (senior staff responsible for the protection of patients' data).

The guidance says that all referrals should use a standard national form with appropriate security and confidentiality applied including when sending to other organisations. Any information shared should be necessary and proportional.

The North Cumbria Integrated Care NHS Foundation Trust also cites its Safeguarding system as the mechanism to store data. The James Paget University Hospital guidance cited *Ulysses* as the database for recorded referrals, with reports sent to the clinical commissioning group and the Department of Health and Social Care. An online search indicates that other NHS trusts also use this programme. One can reasonably assume that similar programmes will be used to record the data if *Ulysses* is not used.

PREVENT IN EDUCATION

How information is managed

At the time of writing, eight schools out of those contacted replied to FOI requests and none had a Prevent or Channel-specific data sharing agreement; all indicated that data is shared on an ad hoc basis, in line with the school data sharing and retention policy, where appropriate.

Where retention policies were given, all indicated that the data would be held until the child's 25th birthday and that the data is held in general safeguarding databases, accessible by safeguarding or pastoral officers, as well as senior staff, where appropriate.

Data sharing agreements

Two colleges also replied to the FOI request, indicating similar arrangements – ad-hoc sharing arrangements, in line with their overall safeguarding policy.

Of the two universities that replied, one did not have a data sharing agreement, as it had not made any Prevent referrals. The other had a short data sharing agreement, which specified that sharing was done under the auspices of section 26 of the Counter-Terrorism and Security Act 2015. The partners to this agreement include:

a) London Borough of Hillingdon

b) Higher Education/Further Education Regional Prevent Coordinator(s)

c) Metropolitan Police Service

d) Local Channel Panel

e) Brunel Pathway College[88]

88 Brunel University London Prevent Policy 2022 (Annex A).

What data is monitored

The University policy outlines both information sharing and collection. It indicates that internet traffic using university networks is monitored, including on personal devices, and that persons accessing sites that breach the acceptable use policy may be reported to the appropriate authorities.

Data storage

Referrals to Prevent are first stored on the University's APEX database. Further information after a referral is raised is collected in conjunction with the Head of Security and Emergency Planning. The Prevent officer and Head of Security and Emergency Planning then decide if the case should be escalated to the local authority.

While the policy states that data is retained for no longer than needed, the retention policy is not freely available. The process for referrals does not make it clear whether consent is sought for a referral – while the policy states that consent should be sought 'wherever possible'.

INCONSISTENT DATA SHARING PRACTICES

Lawful bases

The legal basis for sharing data under Prevent is statutory.

The legislative framework relied on and detailed in documentation – including as cited within Prevent and privacy policies and data sharing agreements – varies. However, they have included the following:

- **Borders, Citizenship and Immigration Act 2009, section 55**[89]
- **Care Act 2014**[90]
- **Children's Act, sections 11 and 16(H)**[91]
- **Children and Social Work Act 2017**[92]
- **Civil Evidence Act 1995**[93]
- **Common Law Powers of Disclosure**[94]
- **Counter-Terrorism and Security Act 2015**[95]
- **Counter-terrorism and Border Security Act 2019, section 20**[96]
- **Crime and Disorder Act 1998, section 115**[97]
- **Data Protection Act 2018**[98]

89 Department for Education (2018). Information sharing Advice for practitioners providing safeguarding services to children, young people, parents and carers (Annex A).

90 Derby City Council (2019). Derby and Derbyshire Safeguarding Children Partnership (Annex A).

91 Ibid.

92 The London Borough of Camden Council Prevent and Channel Panel Data Sharing Agreement (Annex A).

93 Information Sharing Agreement between The University of Lincoln Students' Union and Lincolnshire Police.

94 Ibid.

95 The Counter-Terrorism and Security Act 2015 forms part of the lawful justification for most bodies and is cited in the Channel Duty Guidance issued by the Home Office https://assets.publishing.service.gov.uk/media/651e71d9e4e658001459d997/14.320_HO_Channel_Duty_Guidance_v3_Final_Web.pdf.

96 The London Borough of Camden Council Prevent and Channel Panel Data Sharing Agreement (Annex A).

97 Ibid.

98 The Data Protection Act 2018 forms part of the lawful justification for most bodies.

- **Education Act, section 175**[99]
- **Education and Skills Act 2008, section 74**[100]
- **Higher Education Act 2004**[101]
- **Human Rights Act 1998, article 8**[102]
- **Licensing Act 2003**[103]
- **Limitations Act 1980**[104]
- **The Localism Act 2011**[105]
- **Local Government Act 1972, section 111**[106]
- **Local Government Act 2000**[107]
- **Mental Capacity Act 2005**[108]
- **National Health Service Act (NHSA) 2006**[109]
- **Offender Management Act (OMA) 2007, section 14**[110]
- **Police and Criminal Evidence Act 1984**
- **Protection of Freedoms Act 2012**
- **Rehabilitation of Offenders Act 1974**[111]
- **Terrorism Act**[112]
- **UK General Data Protection Regulation (GDPR), article 6**[113]

In addition, overarching policy documents, such as the Channel Duty Guidance, local safeguarding handbooks, the Child Protection Information Sharing programme and MOPI are referenced for best practice.[114]

Professional guidance is also often invoked as needing due consideration, including:

- **Common Law Duty of Confidence**[115]
- **Caldicott Guardian Principles.**[116]
- **Department of Health Code of Practice on protecting the Confidentiality of service user**[117]

---

99 The London Borough of Camden Council Prevent and Channel Panel Data Sharing Agreement (Annex A).

100 Department for Education (2018). Information sharing Advice for practitioners providing safeguarding services to children, young people, parents and carers (Annex A).

101 Lincolnshire Police (2022). Information Sharing Agreement between The University of Lincoln Students' Union and Lincolnshire Police (Annex A).

102 The London Borough of Camden Council Prevent and Channel Panel Data Sharing Agreement (Annex A) and others.

103 Lincolnshire Police (2022). Information Sharing Agreement between The University of Lincoln Students' Union and Lincolnshire Police (Annex A).

104 Information Sharing Agreement between The University of Lincoln Students' Union and Lincolnshire Police (Annex A).

105 The London Borough of Camden Council Prevent and Channel Panel Data Sharing Agreement (Annex A).

106 Practical Guidance on the sharing of information and information governance for all NHS organisations specifically for Prevent and the Channel process (Annex A).

107 Ibid.

108 The London Borough of Camden Council Prevent and Channel Panel Data Sharing Agreement (Annex A).

109 Ibid.

110 Ibid.

111 Lincolnshire Police (2022). Information Sharing Agreement between The University of Lincoln Students' Union and Lincolnshire Police (Annex A).

112 James Paget University Hospitals (2019). Prevent Policy (Annex A).

113 UK GDPR is a common, article 6 is a common exemption cited.

114 Purpose Specific Data Sharing Agreement (DSA) For the Channel Panel Between MPS and London Borough of Tower Hamlets (Annex A); Prevent and Channel Process in the NHS: information sharing and governance (Annex A).

115 Practical Guidance on the sharing of information and information governance for all NHS organisations specifically for Prevent and the Channel Process; Prevent and Channel Process in the NHS: information sharing and governance; Data-sharing agreement for use in compliance with Prevent statutory duty under counter-terrorism and security act 2015 (Annex A).

116 Practical Guidance on the sharing of information and information governance for all NHS organisations specifically for Prevent and the Channel Process; Prevent and Channel Process in the NHS: information sharing and governance (Annex A).

117 Practical Guidance on the sharing of information and information governance for all NHS organisations specifically for Prevent and the Channel process (Annex A).

- **London Child Protection Procedures 2022**[118]
- **Working Together to Safeguard Children 2018**[119]
- **University of Lincoln Students' Union Safeguarding Children and Vulnerable Adults policy**[120]

BOX 10

THE CALDICOTT PRINCIPLES

In 1997, a committee chaired by Dame Fiona Caldicott reviewed the transfer of patient identifiable information within the health service resulting in a set of standards named the Caldicott Principles. These standards – which can also be used to transfer data across other agencies – were reviewed in 2013 in light of the digitalisation of health information.

The seven Caldicott Principles relating to the use of patient-identifiable information are:

1. **Justify the purpose(s) of using confidential information**
2. **Only use it when absolutely necessary**
3. **Use the minimum that is required**
4. **Access should be on a strict need-to-know basis**
5. **Everyone must understand his or her responsibilities**
6. **Understand and comply with the law**
7. **The duty to share information can be as important as the duty to protect patient confidentiality**

Information sharing protocols

The decision on the lawful basis to share any personal data must be recorded in some form and data sharing agreements are currently considered best practice. Data sharing agreements lay out how information is shared between entities with agreed uses, retention and storage periods and deletion processes. They may also be called information sharing agreements or service level agreements but they serve the same purpose. Councils may also have a Memorandum of Understanding with the Home Office to serve the Channel process.[121]

Murky data sharing practices

The lawful basis of any information sharing should occur on a case-by-case basis. Generally, there will be differing agencies with which a local authority Prevent team or police force will share information. However, some councils do not establish what that sharing map looks like.

For instance, Brighton and Hove City Council only referenced the overarching Channel Guidance on information sharing protocols with respect to Channel cases. Also, in response to an FOI request issued by Defend Digital Me, Brighton and Hove claimed that information was exempt as city-specific information on referrals could constitute information that will reveal where counter-terrorism efforts are most concentrated and present a threat to national security.[122]

Compliance with FOI requests on the same questions has been patchy as some claim an exemption while others are transparent about data sharing practices.

118 Lewisham Borough Council Prevent and Channel Panel Data Sharing Agreement (Annex A).

119 Lincolnshire Police (2022). Information Sharing Agreement between The University of Lincoln Students' Union and Lincolnshire Police (Annex A).

120 Ibid.

121 Practical Guidance on the sharing of information and information governance for all NHS organisations specifically for Prevent and the Channel process (Annex A).

122 Brighton and Hove FOI response (Annex A).

Partners with whom information is shared

Partners with whom information could be shared:[123]

- Police
- Local authority
- Fire service
- Channel panel
- Counter-terrorism Policing – National Headquarters
- National Probation Service
- Community Rehabilitation Company
- Education providers
- Health agencies (trusts, hospitals, clinical commissioning groups)
- Home Office
- OFSTED
- Children's & Adult Social Care
- Other relevant internal departments
- Other public bodies
- Home Office-approved intervention providers
- Third sector/voluntary commissioned service providers
- Other central government departments
- Schools and colleges
- Other local councils
- Children's Social care
- Early Help
- Multi Agency Safeguarding Hub (MASH)
- Housing
- Family Justice Centre
- Metropolitan Police Service, British Transport Police, City of London Police, Frontline Policing (e.g. local police)
- Counter-Terrorism Command (e.g. SO15)
- Immigration
- HM Courts and Tribunals Service
- Children and Family Court Advisory and Support Service
- Children and Adolescent Mental Health Services
- Domestic violence advocates
- Multi-agency risk conferences
- Women's centre, rape and sexual abuse support services
- Teams supporting children with disabilities
- Local authority dedicated officers
- Higher education and further education regional Prevent coordinator
- HM Prison and Probation Service
- Office for Security and Counter-Terrorism Joint Extremism Unit (JEXU)
- Prisons
- Youth offending teams
- Businesses e.g. security companies, suppliers of goods and services, third-party processors, private-sector organisations working on anti-crime strategies with police forces
- Partner agencies working on crime reduction or safeguarding initiatives, agencies and third parties concerned with the safeguarding of and investigation of international and domestic national security
- HM Revenue and Customs
- Coroners
- The Serious Fraud Office
- The Child Maintenance Service
- The National Fraud Initiative and private safeguarding agencies
- Police and Crime Commissioners

123 These partners have been cited within FOI responses noted in Annex A.

- **Ombudsmen, auditors and regulatory authorities**
- **Any body where required under any legislation, rule of law, or court order actuarial valuers and pension providers**
- **Other bodies or individuals where necessary to prevent harm to individuals**
- **The media, including public disclosures via social media**
- **The insurance industry**

The wide-ranging list of organisations does not imply that each will receive information as each disclosure must be judged case by case – and the above list includes partners with whom information is shared for the Channel panel – but lack of specificity within some privacy notices and agreements implies that any such organisation could receive information.

Information shared

Type of information that could be shared includes:[124]

- **Demographics (name, date of birth, gender, address, ethnicity)**
- **Offending history**
- **Living arrangements**
- **Family and personal relationships**
- **Statutory education**
- **Neighbourhood**
- **Emotional and mental health**
- **Perceptions of self**
- **Thinking and behaviour**
- **Attitudes to engagement in relevant activity**
- **Lifestyle substance misuse**
- **Motivation to change**
- **Cultural factors**
- **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**
- **Data subject and family's legal status**
- **Accommodation**
- **Employment status**
- **Physical and emotional well-being and parenting**
- **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 provided 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**
- **Information such as court orders and professional involvement**
- **The data subject and immediate families' immigration history**
- **Police audio and video recording**

124 The breadth of information that could be shared has been disclosed by FOI responses cited in Annex A.

- **Documents sent relating to the data subject e.g. referrals received from other agencies and professionals**
- **Political opinions**
- **Religious or philosophical beliefs**
- **Sex life/sexual orientation**
- **Data from police databases**
- **Externally shared data that is anonymised e.g. for research**
- **Online activity**

Sharing of this data will only occur if deemed necessary to inform the referral. For instance, Camden's Prevent and Channel Panel Data Sharing Agreement states that "understanding a data subject's ethnic origin, political opinions and religious/philosophical beliefs will enable the panel to assess whether the ideas, beliefs and language used by a data subject are extremist in nature and where their influences may have occurred.

Similarly, the sharing of data including health and sex life/orientation will support the panel in making informed decisions about the best approach to safeguard the individual (e.g. the impact of substance misuse on their vulnerability."[125]

Sensitive data – such as ethnic origin – can only be shared if sections 35(4)[126] and 35(5)[127] of the Data Protection Act 2018 are satisfied i.e. if there is consent or a law enforcement purpose with a policy document needed in both cases.

Sharing considerations

Some agreements state the need to consider anonymisation of information where possible, for example, referring to "a young person" without giving the individual's name, address or information,[128] or pseudonymised.[129] However, most concede this type of anonymisation is impractical and if pseudonymised, due to other personal data held within the records, the subject could be re-identifiable when that data is combined with other data sources.

Each piece of information should be evaluated against necessity and proportionality criteria.

Governance challenges

The extent of the sharing can be broad and sharing arrangements can extend well beyond one local authority with regional Prevent hubs formed. Therefore, for example, if information is being shared with the clinical commissioning groups, it could mean several clinical commissioning groups covering different boroughs – this is sometimes explicit in the agreement and at other times not.

Bodies party to the agreement could be using voluntary or other service providers and the risks can include onward sharing by third parties.[130]

Organisations mentioned in the data sharing agreements are also not necessarily specific in that they detail the types of bodies the data may be shared with and therefore, there may not be any assessment.[131]

---

125 Prevent and Channel Panel Data Sharing Agreement. Camden Council (Annex A).

126 Section 35(4) of the Data Protection Act 2018 states that lawful and fair processing, when the data is sensitive includes when: (a) the data subject has given consent to the processing for the law enforcement purpose as mentioned in subsection (2)(a), and (b) at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

127 Section 35(5) of the Data Protection Act 2018 states that lawful and fair processing, when the data is sensitive can also include when: the processing is strictly necessary for the law enforcement purpose, the processing meets at least one of the conditions in Schedule 8, and at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

128 Memorandum of Understanding Lancashire and Cumbria Channel Process (Annex A).

129 Tower Hamlets (2020). Purpose Specific Data Sharing Agreement (DSA) For the Channel Panel Between MPS and London Borough of Tower Hamlets. FOI disclosure as per Annex A.

130 The London Borough of Camden council Data Protection Impact Assessment (Annex A).

131 The London Borough of Camden Council. Prevent and Channel Panel Data Sharing Agreement (Annex A).

In some cases, there is a single point of contact with names to contact under the sharing agreement but that is not a universal feature.[132] Some agreements also mention that sub-processors cannot be used. However, others don't mention such use, nor the use of any third-party software or apps.

Onward sharing risks could extend to cross-border sharing – but there is ambiguity within documentation if overseas sharing might occur or not. For instance, for one council, the DPIA bars cross-border sharing and the data sharing agreement states that sharing remains in the UK; however, further along in the data sharing document it states that sharing won't extend beyond the European Economic Area, an area that encompasses more than the UK.[133]

Some agreements also have stipulated that any partner with whom information is shared should have a written privacy policy. However, this is not universally true and the parameters or requirements set by the policy are not necessarily made clear.[134]

In the case of a Channel panel, note-taking and individual file creation serve as another area in which the sharing of information is unclear. The stipulations around who can take notes and when are inconsistent across geographical areas as are those regarding storage and retention periods. Retention periods for information may be mentioned in policy documents and agreements but they are not consistent across all the bodies.[135]

Data sharing expectations

In practice, this creates an issue when individuals who have been referred to Prevent ask about data that has been shared as the responses tend to assume that data has not been shared with other agencies who were for example present in a Channel panel or multi-agency safeguarding hub (convened to share information to safeguard children) meeting.

In the case of Amina in **Box 11**, numerous agencies and individuals were present in the strategy meeting discussing her case and their own internal practice must have generated data and notes about the individual and these may have been stored on databases in their own management systems. It would be a colossal task to find and retrieve all these entries before any data rights can be requested, such as rectification or deletion.

132 Assessed from the documents analysed from Annex A.

133 The London Borough of Camden Council. Prevent and Channel Panel Data Sharing Agreement (Annex A).

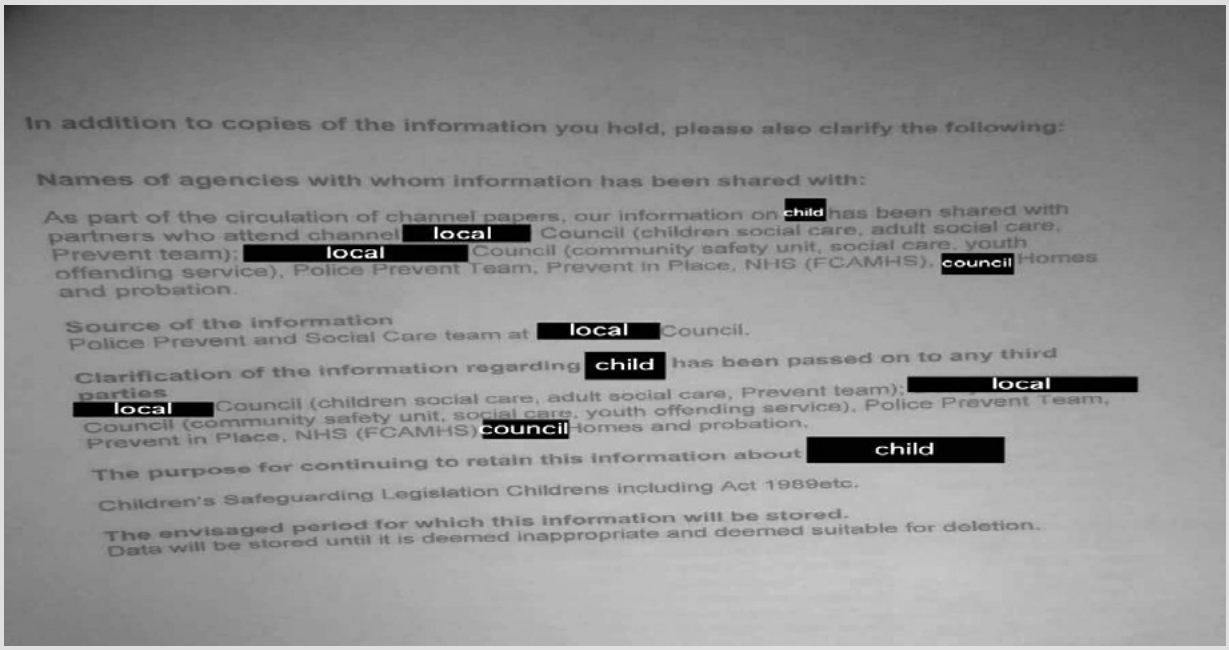
134 Assessed from the documents analysed from Annex A.

135 Assessed from the documents analysed from Annex A.

BOX 11

CASE OF AMINA

Amina had requested her young primary school child's data after a Prevent referral and found that a number of third parties had received her child's information and data without her consent or knowledge. The following is an excerpt from the answer she received to her SAR:


In addition to copies of the information you hold, please also clarify the following:

Names of agencies with whom information has been shared with:

As part of the circulation of channel papers, our information on child has been shared with partners who attend channel local Council (children social care, adult social care, Prevent team); local Council (community safety unit, social care, youth offending service), Police Prevent Team, Prevent in Place, NHS (FCAMHS), council Homes and probation.

Source of the information
Police Prevent and Social Care team at local Council.

Clarification of the information regarding child has been passed on to any third parties
local Council (children social care, adult social care, Prevent team); local Council (community safety unit, social care, youth offending service), Police Prevent Team, Prevent in Place, NHS (FCAMHS) council Homes and probation.

The purpose for continuing to retain this information about child

Children's Safeguarding Legislation Childrens including Act 1989etc.

The envisaged period for which this information will be stored.
Data will be stored until it is deemed inappropriate and deemed suitable for deletion.

For a data subject to understand where their data has been shared may prove difficult in light of different policies around data processing and recording information. For instance, Brunel University states that "a record of each shared event, to include the date, the name of the organisation with which the data have been shared, and details of the transaction, will be securely retained by the University Prevent Coordinator for one year after the date on which the information was shared." However, as we have established that shared information can be retained for six years and beyond on other systems including police databases.[136]

Divergent data sharing agreements

As local authorities are able to use their own processes to meet their obligations under Prevent, there is some divergence in practice. This is most pronounced where structural differences within the Prevent system lead to Home Office oversight and funding differences.

There have been some efforts to form umbrella practices to be adopted across areas.

For example, Dovetail pilot participants signed onto an Umbrella Memorandum of Understanding – between the Home Office and participating council. The London Office of Technology and Innovation also drafted a pan-London data sharing agreement that some London councils have opted into using.

Neither of the mentioned multi-area agreements has sought partners such as NHS Trusts, clinical commissioning groups,

136 Brunel University Prevent Policy (Annex A).

colleges, universities or schools outside council control to sign onto the agreements, despite their being subject to the Prevent Duty.

The Umbrella Memorandum of Understanding specifically states that some sharing of data outside of the agreement may be needed but risk and contingencies must be considered in each case.[137]

Other areas – such as Devon & Cornwall, have in place information sharing agreements[138] between a wider set of partners to including the local constabulary, NHS Trusts, clinical commissioning, the National Probation Service and the Fire and Rescue Service (not schools or universities). The agreement sets out in some detail how, why and who the data is shared with for more than just the Prevent strategy and apparently intended for a wide range of policing purposes.

Some bodies – e.g. Lincolnshire Police – have separate information sharing agreements for specific processes, covering Prevent and Channel information gathering, the Channel panel and then agreements between them and the University of Lincoln and with its Student Union.[139]

CONSENT AND TRANSPARENCY UNDER PREVENT

Consent is neither needed nor sought under the Prevent duty, which means that the referee, or in the case of a minor, their parents or guardian, will not necessarily know they have been referred. This lack of knowledge means that individuals or a family could be targeted without understanding why, such as in the case of Sofyan's mother in **Box 12**.

It also means that those processing the data, such as parties to a data sharing agreement as well as those with statutory obligations under the Prevent Duty, are in positions of power over data subjects and data subjects have little or no control over why and how their data is processed. The impact of this can extend to children as young as seven and even younger.

The rationale for sharing the data of children so young was explained in one data sharing agreement in the following excerpt:

It is, however, 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.

However, children under the age of 7 are unlikely to be able to critically think which may result in them being more susceptible to extremist views of those around them. The majority of referrals to Channel are for vulnerable individuals (both children and adults).[140]

137 The North Cumbria Integrated Care NHS Foundation Trust within the jurisdiction of the agreement responded to Lewis & Klein Associates Ltd's FOI request, acknowledging they did not have any data sharing agreements in place, despite being bound by the Duty.

138 Devon and Cornwall Police (2020) Devon and Cornwall Partnership Information Sharing Agreement. Para 1.1 – 1.2

139 Information Sharing Agreement between The University of Lincoln Students' Union and Lincolnshire Police (Annex A)

140 Prevent and Channel Data Sharing Agreement. Camden Council. Annex A

BOX 12

CASE OF SOFYAN

Sofyan is a nine-year-old Muslim boy based in London, in year 5 of a primary school that is part of a Prevent Priority Area (one which receives additional funding for Prevent projects). Sofyan's mother was concerned because she was being contacted regularly for meetings for very low level disruption and 'rough play' that could easily be dealt with by the school and that the language being used to describe Sofyan's misbehaviour was loaded with terms around radicalization.

In 2019, Sofyan's mother was informed that 'external agencies' had been contacted due to a concerning incident. Within a few days, Sofyan's mother was approached by children's services who made a visit to her home and conducted a section 17 assessment. Sofyan's mother was not given information prior to the visit to explain what the section 17 assessment was, that it was voluntary, nor how the section 17 had been provoked, in this case, off the back of a Prevent referral.

Following the assessment, Sofyan's mother sought support from Prevent Watch and asked the social worker for a copy of the full assessment and for the reasons why the assessment had been carried out. The social worker confirmed that concerns had been raised by the school to Prevent and consequently to social services.

If Sofyan's mother had not pursued the information she may have never known that such information was shared as even though the school flagged that a referral had been made, they only said it was made to unspecified external agencies. That could have meant anything and was disclosed only after the fact and not as part of seeking consent.

Complications around safeguarding

Issues around consent get murkier when organisations view the Prevent Duty through the lens of safeguarding as seeking consent is the gold standard in terms of justifying sharing information or referrals.

The City of London Prevent Policy[141] for instance states:

Before making a referral, practitioners should respond as we would to all concerns, by clarifying the information. For children this will involve talking to the child/young persons and their parents or legal guardian (unless the family is implicated in potential extremism) and to other professionals working with the child/young person. Any referral should be made with the young person/ family's knowledge and consent, unless to do so would place the child/young person at risk of harm. For adults (over 18 years old) practitioners should seek the consent of the person who may be at risk of extremism or radicalisation before taking action or sharing information. In some cases, where a person refuses consent, information can still lawfully be shared if it is in the public interest to do so. This may include protecting someone from serious harm or preventing crime and disorder.

Other data sharing agreements may also indicate that consent might be sought from individuals before their data is shared although caveats such as "where is appropriate or insofar possible" are used as well.[142]

Consent for Channel

The Dovetail pilot participant Blackburn with Darwen's practices illuminates transparency for the one stage where obtaining consent is mandatory: when a Channel intervention is offered.

Once a referral receives a visit from a member of the Channel Team, they will provide them with a leaflet with information about Channel and how their data will be used.

141 Listed in Annex A.

142 Information sharing arrangement between LSE and police (Annex A).

The leaflet states that Channel is a voluntary, non-criminal intervention and that data might be shared with other safeguarding services. It also states that data is stored on local authority servers and a Home Office case management system (Channel Management Information System).

The leaflet does not mention the other databases that Prevent-related information will likely be stored on, including other police or health databases. It does not state that data can be requested to be deleted, not what happens if an intervention is refused.

A more comprehensive consent form is provided for those persons who assent to an intervention. It states that information will be held for as long as the law or business necessity allows, that data can be shared with multiple agencies and that confidentiality may not be maintained if there is a significant concern.

The leaflet and the form provide a link to the Blackburn with Darwen privacy notice, which further outlines that data will be collected, who it might be shared with and how long it will be held.

The consent form is the same for children and adults, with adults providing consent for children. The form gives the following data retention timelines, with no indication of how the different categories are decided:

*** 6 years Adults**

*** Up to 18th birthday Level 1**

*** 25 years after 18th birthday Level 2**

*** 99 years All others**

Preventing scrutiny

Information requests relating to Prevent referrals tend to come up against exemptions making it difficult to scrutinise both individual data and border statistics. For instance, an FOI to Brighton and Hove City Council seeking statistics around onward sharing of Prevent referrals elicited the following response:

Disclosing onward sharing would by default reveal the number of referrals in the city. Disclosure of this information would potentially reveal the identity of areas where the threat to the national security of the UK is greatest. More crimes may be committed should criminals begin to grasp each Councils specific statistics in respect of the Channel programme, particularly if mosaic requests are received by each Council. Releasing this information would enable terrorists or criminals to gain knowledge about where counter-terrorism, law enforcement and public safety measures are focussed and thus risks effective targeting of individuals, organisation and areas with their radicalisation efforts. This may impact negatively on the delivery of Prevent, and on the range of activities deployed to prevent terrorism.

Questions also arise as to whether Prevent referees are the subject of unlawful scrutiny during the period they remain on the database. This raises concerns that during that period, they will be the subject of secret surveillance.

While the existence of and grounds for surveillance are beyond the scope of this report, it is worth noting that there is case law that accepts some surveillance is necessary for a democratic society in the interests of national security or for the prevention of disorder or crime.[143] However, powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the European Convention of Human Rights only insofar as strictly necessary for safeguarding democratic institutions. Further case law outlines when grounds for Article 8 infringements can be made.[144]

143 Klass and Others v Germany; Szabó and Vissy v. Hungary.

144 Roman Zakharov v. Russia [GC], § 227; Szabó and Vissy v. Hungary, § 54; Kennedy v. the United Kingdom, § 130.

Most referrers will probably not appreciate as well that two potential pathways await a referee should the gateway assessment not lead to an NFA status – multi-agency or police-led process. The latter is a process where Channel or a deradicalisation intervention is no longer a potential outcome and sits within a covert space subject to separate data protection rules, as referenced in section two of the report – The UK Legal Framework for Data Protection. The fact that the Prevent Case Management Tracker is managed by Counter-terrorism Police with referrals passing through intelligence actors makes Prevent subject to the covert space where it is unclear where and if there is any parliamentary scrutiny.

ANALYSIS

Necessity and proportionality

Prevent referrals have stirred controversy in their own right but a fresh look at how personal data moves through several institutional layers and the governance around that system demonstrates how proportionality and necessity requirements are being stretched.

Too wide a net

Critics of the policy have already argued that the broad signs officials, such as teachers, are encouraged to look out for[145] cast too wide a net on so-called 'pre-terrorists'.

The case studies reviewed in this report show how natural curiosity, remarks around religion or even a keen interest in history can get construed as suspicious enough to warrant a Prevent referral.

Similarly, suspicions raised about associates or family members can embroil young children in Prevent. These should not be considered isolated cases; Prevent referral statistics and the ratio of actual referrals that show signs of radicalisation[146] show that the threshold for intervention or threat of radicalisation is not being met. This throws into doubt whether there is indeed a valid policing purpose for the retention of the Prevent referral data.

Excessive data retention

The police's guideline for retaining information for Prevent states there has to be a six-year minimum retention period but this is based on guidance that was not intended for pre-crime interventions such as Prevent. There have never been guidelines specific to Prevent and the police's rationale for data retention has relied on the risk of

145 Preventing Education? Human Rights and UK Counter-Terrorism Policy in Schools. Rights and Security International (2016) https://www.rightsandsecurity.org/assets/downloads/preventing-education-final-to-print-3.compressed-1_.pdf; Is the Prevent Program Racist? Amnesty International UK (2022) https://www.amnesty.org.uk/blogs/campaigns-blog/prevent-program-racist

146 False Positives: the Prevent counter-extremism policy in healthcare. Medact (2020) https://www.medact.org/2020/resources/reports/false-positives-the-prevent-counter-extremism-policy-in-healthcare/

"re-offending". However, in the first instance, no offence would have ever been committed.

In some cases, such as Noah (Box 8), where the subject was briefly added to a chat group connected to terrorism, there were strong indications that the data would be retained according to the highest retention level, meaning until the subject reaches the age of 100, with a review every 10 years. Such excessive retention periods are neither necessary nor proportionate. The highest thresholds of proportionality are necessary for personal data that extends to religious beliefs, medical data and other confidential information; the more intrusive the data, the higher the threshold this proportionality test must apply.

Conflation of victim and perpetrator

The reasons for retention are further confused as policy language and protocol conflate perpetrator and victim. The purpose of Prevent, the police tell family members, is to protect individuals because they are vulnerable, yet they are processed in police databases and regularly referred to as a national security concern.

The adoption of ambiguous terminology, such as "nominals", reminiscent of other pre-crime measures, such as the flawed Gangs Matrix,[147] further conflates the status of referees as victims or supposed perpetrators.

Prevent confused with safeguarding

We do not believe that there are grounds to retain Prevent data but it is not only retained but shared. While consent is not sought under Prevent, sometimes dual processes are in play that intertwine social services' involvement and safeguarding issues with Prevent. The issue of when and how consent is necessary then becomes confused as different rules and considerations apply.

Professionals involved in referrals to Prevent will have responsibilities that might impact on decisions about data and professional discretion will kick in.

For example, the common law duty of confidentiality means medical professionals may or may not override legal duties to share data as they see it impacting on their ability to deliver health care. Those tensions are apparent in other professions where Prevent is mandatory and the ICO or police may not be the best authority to help navigate the line between profession and de facto police.

Unclear statutory thresholds

The data of other household members is also often shared as part of a subject's referral but it is unclear if a separate decision is made for the lawful basis for sharing of this data as these should be made on a case-by-case basis.

The most commonly cited law for Prevent and the lawful basis for data processing is the Counter-Terrorism and Security Act 2015. However, various other pieces of legislation have formed the framework relied on to share data. How the threshold criteria vary according to various statutes is not clear. As a result, there appear to be several gaps in guidance around how Prevent data is treated.

Purpose limitation

Where Channel referrals were not taken forward, police documents indicated that the police with partners can undertake a wide range of disruptive measures, which takes place after a section 36 decision is made.

Those making a referral may believe that the information goes to the council through the multi-agency process rather than being aware that, in the first instance, all referrals enter a covert security space, undergoing 'deconfliction' by a Fixed Intelligence Management Unit and then a police gateway assessment by a counter-terrorism case officer. Those assessments determine the paths of the referral, including whether it will go through the Channel process

147 The Metropolitan Police Service was ordered to 'wholesale change' the database it ran on individuals vulnerable to gang violence as it breached people's right to privacy with Black people disproportionately represented on it: Liberty (2022). Met to overhaul 'racist' gangs matrix after landmark legal challenge https://www.libertyhumanrights.org.uk/issue/met-to-overhaul-racist-gangs-matrix-after-landmark-legal-challenge/

led by local authorities, or remain in the covert space under a police-led process.

If the lawful basis of collecting information is to determine if they meet the threshold for Channel, then activity in lieu of that under a police-led partnership indicates the reuse of data collected for Prevent for law-enforcement purposes. It is not clear how this is governed and whether this meets guidelines for data management.

For non-law enforcement authorities, purpose limitation of Prevent data is particularly important but if a school has referred someone to Prevent as a legal obligation under the Counter-Terrorism and Security Act 2015 and that referral has ended up being used to exclude someone from school or is passed on to another body via a multi-agency safeguarding hub, then there could be a breach of purpose limitation under data protection law.

Also, if notes around Prevent are scanned into NHS records and become health data, that could indicate unlawful reuse of data again.

Unclear data processing map

The referral process and case studies reveal that data could be held at every point of the referral system, including by the referring institution. Once a referral passes to the Counter-Terrorism Policing Prevent team then the data attached to it could be shared widely under separate processing protocols and it is unclear when the police deem it "necessary" to remove the data and if deletion from one system leads to deletion from another police system.

Whenever data is shared, the applicable lawful basis should be recorded, which raises the question of whether checks made for Prevent referrals also leave a record on the database and if those traces factor into any future police decision-making.

Where multi-agency processes kick in, data sharing agreements are not always in play and when they are, templates differ from region to region. At the information gathering phases for Channel, some local authorities only reference the overarching Channel guidance to indicate how they share information so the identity of the main bodies with whom they share information is not clear.

The lawful basis of any information sharing should be identified on a case-by-case basis and each decision should be recorded. However, potentially, that data can then be shared with any agency – or obtained from any agency – based on a simple subjective assessment of whether the decision to do so is warranted.

When there are data sharing agreements in place, the net of agencies within the overall ecosystem is also not necessarily confined. There are onward risks regarding the protocols any receiving agency applies to further sharing.

Prevent data sharing harms

The bottom line is that we know data sharing occurs and that these arrangements have not been declared openly to the individuals concerned. There are agreements between further education and higher education institutions, and sharing between these institutions has resulted in significant harms to young people's lives.

The potential impact does not stop at education – what is the impact if the person being referred is awaiting a decision on refugee status or residency? This is particularly relevant given the new duty guidance that will come into effect in January 2024, which takes into account the recommendation of extending Prevent to the front line practitioners of the border force and immigration.

There are also many unanswered questions around the implications of holding a person's data on so many systems or the potential for data matching and whether they could be disproportionately subject to further police actions, such as stop and search or Schedule 7 powers under the Terrorism Act 2000 that allows questioning at ports and borders, another policy only revealed through accidental disclosure.[148] Those concerns

148 Harassment at Borders – The impact on the Muslim community. CAGE (2019) https://www.cage.ngo/product/schedule-7-harassment-at-borders-report

resurface when we consider that sharing occurs up to the level of the Home Office[149] and could be included in cross-border data sharing.

Patchy retention and storage protocols

Prevent referrals – particularly when applied to children – can also be subsumed within other safeguarding processes, and subject to those processes, protocols, forms, databases, recording standards and retention periods, which may or may not align when Prevent is added.

Data retention and storage occurs across the institution, local authority and Home Office levels but the protocols across these three levels are less clear. Many of these agreements also acknowledge that there will be instances where it is *not reasonable* to require third parties to delete data where it is too difficult or time-consuming to do so.

No inherent right to erasure

Very few agreements outline the process for compliance with the right to erasure. Those documents that mention it give limited information on how compliance will be assessed, except to say it is the responsibility of the data controller to assess whether erasure requests will be complied with.

As such, data controllers must correct or erase incorrect or misleading data as soon as possible, acknowledge it as a mistake and carefully consider any challenges to the accuracy of personal data.

Considering the expansive web in which data could be shared, that would require each person to establish whom data was shared with and file individual requests to get it removed. It, therefore, becomes too onerous for an individual or their family to exercise their rights to object, rectification or erasure, the pursuit of which often requires legal action at personal expense.

Privacy notices retrieved appeared generic with only Blackburn with Darwen utilising a clear and detailed form that Prevent referees would receive when assenting to a Channel intervention. Some information available in privacy notices was also too complex to be deemed appropriate, especially for vulnerable persons or children.

Individuals on the Prevent database in the 'no further action' camp will still not be informed of that processing. The Home Office considers its online privacy notice to be adequate information but it is unreasonable for persons unaware that their data has been collected to view specific privacy notices online.

No lawful basis

In the case of errors and Prevent referrals based on unfounded suspicion, there has been success in the courts invoking data protection and human rights benchmarks. For instance, when solicitors Deighton, Pierce and Glynn took action in relation to the retention of an 11-year-old child's data under Prevent, the retention was ruled unlawful because the law enforcement purpose had to be lawful and fair. A 2020 report by Medact[150] deducted that 95% of Prevent cases do not meet current thresholds for there to be any threat of terrorism or radicalisation. The latest figures, show this is at least 84%. It is therefore questionable whether there is a lawful purpose to any retention of this data.

The court also found that the Metropolitan Police Service underestimated the impact of Prevent data retention and sharing on a child's privacy rights and that there was a continuous fear of his data being shared with third parties based on views and statements he was alleged to have made when he was 11 years old. It also ruled that there was no guarantee the data would not be shared. The ruling presents a damning indictment on the lawful basis for police retention of Prevent data and that there is in fact a policing purpose at all in the majority of cases.

149 Data Sharing Agreement between Counter-terrorism Policing South East [and others] (Annex A). London Borough of Camden Council. Data Protection Impact Assessment (Annex A).

150 False Positives: the Prevent counter-extremism policy in healthcare. Medact (2020) Medact https://www.medact.org/2020/resources/reports/false-positives-the-prevent-counter-extremism-policy-in-healthcare/

In another case, the Metropolitan Police Service tried to argue a rationale for retaining data due to radicalisation being a process. The judge found no issue with retaining data in principle but said that there had to be legitimate concerns.

Lack of transparency preventing justice

It is our belief that successful challenges would multiply if there were more transparency about when referrals are taking place and with whom. Even FOI requests or subject access requests are tricky, with organisations quick to invoke exemptions.

In the case of the FOI requests we made, some organisations claimed exemptions based on national security, the length of time it would take to comply, or that it would cost too much to retrieve the information. Yet others felt it was completely appropriate to share the information we requested.

That inconsistency does not seem reasonable and shows a patchwork approach to the incredibly sensitive processing of personal data and redress. For its part, the Home Office Umbrella Memorandum of Understanding advocates for transparency but its directive to inform it of any FOI requests suggests further logging of Prevent-related data at the Home Office level.

Weakening safeguards

Opacity around information retrieval extends to personal subject access requests and it is discouraging that proposed data protection reforms will make them more onerous and, in essence, weaken safeguards while further empowering police and state use of data without consent. These changes could add to the existing suite of legislative changes that have already shifted power toward the state in the realm of policing and national security.[151]

The lack of parliamentary scrutiny over Prevent – particularly the police-led partnerships pathway in the covert space – is also a live issue and a question requiring answers from the Home Secretary and Prime Minister.

Disproportionate impact and rights denial

The Prevent policy should be viewed alongside the UK government's evolving approach to counter-terrorism such as that outlined in the controversial "independent review" of Prevent by William Shawcross, whose recommendations will see more emphasis on so-called Islamist extremism. A review of data processing around Prevent already illustrates the diversion from ordinary data protection standards, which means many UK Muslims are already subject to an alternative track on rights.

In other surveillance regimes, there are clear routes for people to request that their information is removed, or to seek redress. It would be possible to create a central mechanism for people to ask for complaints to be handled and data to be removed.

Furthermore in other formal surveillance settings, courts have ruled that people should be notified when they have been surveilled, but this has ceased as the person poses no risk and investigations have ended, so long as notification would not create a risk, such as tipping off. Notifying people whose data has been retained, but are no longer under any suspicion, would help them understand if their data has been potentially misused in order to file complaints, for example. The Court of Justice of the European Union asked for notification in relation to the UK's use of retained Internet records, for instance.[152]

Before the policy is subject to further reform, there must be a complete review as to the overall legality of the Prevent policy.

---

151 Police, Crime, Sentencing and Courts Act 2022; National Security Act 2023; Public Order Act 2023; Nationality and Borders Act 2022

152 *Secretary of State for the Home Department v Watson & Others* [2018] EWCA Civ 70 See https://wiki.openrightsgroup.org/wiki/Secretary_of_State_for_the_Home_Department_v_Watson_%26_Others

RECOMMENDATIONS

The Prevent duty is an example of a pre-crime measure, which impedes human rights and creates a system filled with "false positive" results to determine so-called "would-be terrorists". As such, we recommend that:

1. The government scraps the Prevent Duty to free resources to focus on evidence-based counter-terrorism strategies rather than speculative pre-crime guesswork; it should impose an immediate moratorium on Prevent referrals.
2. The Home Office imposes a blanket ban on the retention of data where thresholds under section 36 of the Counter-Terrorism and Security Act 2015 are not met.

Should the government fail to scrap Prevent and the Home Office continue to retain data even where thresholds are not met, we recommend:

3. The ICO audits the Home Office's Prevent policy and its execution across the various institutions where the processing of personal data takes place, including the applicability of national security exemptions, applied when Prevent falls under a police-led process.
4. The ICO directs data controllers of the Prevent programme to provide guidance to ensure data subjects can track where a Prevent referral has been made for them to execute their right of erasure.
5. Policing bodies review the management of information related to Prevent with stricter deletion rules where there has been no further action.
6. Local authorities, police departments and individual institutions subject to the Prevent duty ensure maximum transparency around referrals, data processing and data sharing practices, including the systems used and in as clear detail as possible.
7. The NHS should ensure that there is no onward sharing of Prevent related data into other platforms and that data is not reused for other purposes.
8. Statistics (aggregated data) should be transparently published to enable scrutiny and support accountability.
9. Data about the number of Prevent referrals, amount of information held and outcomes of referrals should be available on a geographic level to support with demographic information and scrutiny of the programme.
10. The Prevent programme should publish data flows to help people understand how to use their information rights.
11. A clear route for complaints and requests for deletion or review should be put in place
12. Notification of people whose data has been held in the Prevent system but subsequently removed should take place.
13. Guidance to those under the duty should specifically notify them that referral data are passed to intelligence officers for initial assessment and are therefore used in the covert space.
14. Where a decision data crosses a threshold from safeguarding to crime use, or from police to national security use, an independent authority should decide whether the data is to be shared, rather than the decision being an internal police matter. The principle of independent decisions for data use already exists regarding Communications Data under the IPA for example.[153]

153 https://www.legislation.gov.uk/ukpga/2016/25/part/3 and https://www.legislation.gov.uk/uksi/2018/1123/regulation/5

We also invite others to continue to challenge the abrogation of rights occurring under the Prevent policy, including that:

15. The legal community conducts a legal challenge to the lawfulness of the Prevent Duty and its infringements on UK data protection law and Article 8 of the Human Rights Act 1998 – the right to privacy.
16. Individuals should submit subject access requests to determine if they or their child has been referred under Prevent and exercise their right to object, rectification and erasure.
17. Individuals refused their rights escalate their request through the ICO complaint mechanism, a Department of Education complaint or judicial review.
18. Researchers should map the data collection, retention, storage and sharing practices of local areas to determine compliance with data protection laws.
19. The government and political opposition should review Open Rights Group's recommendations around the Data Protection and Digital Information Bill and should support dropping the bill or engaging the amendments to improve safeguards for those entangled in the UK's pre-criminal space.

ANNEXES

Annex A

FOI List

https://docs.google.com/spreadsheets/d/1kmy6yyquXCHPHNJWzo4VYwg2rcD2bdbChpP9U_CQubs/edit?usp=sharing


ORG
OPEN RIGHTS
GROUP