



Domestic Violence Disclosure Scheme (DVDS) Child Sex Offender Disclosure Scheme (CSODS)

Abstract

The aim of both schemes is to provide right type and depth of information where appropriate, so those potentially at risk (or someone best placed to safeguard them) can gain an informed understanding of the subjects' character and the risk they pose, meaning they can make informed decisions about safety and relationships, potentially preventing future crime and abuse.

Policy

1. Introduction

The Domestic Violence Disclosure Scheme (DVDS) and the Child Sex Offender Disclosure Scheme (CSODS) were developed to help safeguard people who are potentially vulnerable due to the presence of someone in their lives with a history of abuse and/or violence. The schemes give direction to police on when and how to lawfully and proportionately share known information relating to risk.

The aim of both schemes is to provide right type and depth of information where appropriate, so those potentially at risk (or someone best placed to safeguard them) can gain an informed understanding of the subjects' character and the risk they pose, meaning they can make informed decisions about safety and relationships, potentially preventing future crime and abuse.

Both schemes require compliance with data protection and human rights legislation. The DVDS National Guidance is specifically underpinned by the [Domestic Abuse Act 2021](#), requiring police to follow the guidance or have a robust rationale for any deviation. The purpose of the legislation and guidance being to ensure that the rights of subjects and previous victims are only breached to the extent needed to achieve the aim, and that personal data is managed lawfully. This means there is no guaranteed right or entitlement for police information to be provided under these schemes, nor is there a requirement for police to provide exhaustive details in relation to any information provided. A series of perquisites must also be met before any disclosure can be given.

The schemes are voluntary for the person potentially at risk, they are under no obligation to either listen to any information provided by police or act upon it. The guidance directs that police should provide support and guidance to those at risk and consider whether further safeguarding actions need to be undertaken.

Whilst there is national guidance and information provided in Authorised Professional Practice (APP), there is a requirement for this policy in order to:

- Explain how the national guidance should be operationally and practically applied.
- Provide clarity on how the aim should be achieved.
- Define roles and responsibilities.
- Explain where it is anticipated there may be deviation from the guidance.

This policy and procedure apply to all Surrey police officers and staff dealing with public contact.

2. Scope

Whilst DVDS and CSODS are intended to deal with very different risks, the legislative considerations, principles and practicalities of the two schemes are almost identical. The risks posed to vulnerable people will often overlap both schemes, for these reasons this policy covers both DVDS and CSODS processes.

This policy is not intended to replace the direction of the national guidance or APP for either scheme. Officers and staff working on specialist teams involved in managing DVDS and CSODS occurrences must familiarise themselves with these documents, as they contain significant further detail, guidance and context.

This policy focuses on core processes and decision points within the schemes, where specific action must be taken. More detailed practical guidance is available in the DVDS/CSODS operational guide.

3. Statement

The aim of this policy is to ensure that Surrey Police:

- Provide a timely, consistent and high-quality response to all DVDS and CSOD occurrences.
- Provide anyone identified as vulnerable (or someone best placed to safeguard them) with the right type and depth of information to ensure they have an informed understanding of the subject's character and offer them the best opportunity to make informed choices about safety and relationships.
- Understand and comply with national guidance provided by the Home Office and the APP and the implications of any deviation.
- Can provide explanation, confidence, and transparency to the Surrey public around how DVDS and CSODS are processed.

Procedure

1. TERMINOLOGY

The national guidance for DVDS labels the key people involved as 'A', 'B' and 'C'. To ensure operational clarity, more simplified language must be used by those dealing with DVDS and CSOD occurrences.

- **Recipient** - Referred to in the DVDS guidance as 'A' – this is the person who is potentially at risk and will normally receive any potential disclosure, unless there is a reason to provide it to someone best placed to safeguard them.
- **Subject** - Referred to in the DVDS guidance as 'B' – this is the person potentially posing the risk.
- **Applicant** - Referred to in the DVDS guidance as 'C' – this is the person making the request, if it is different from the recipient.

2. ENTRY METHODS

2.1 Both DVDS and CSODS have two entry methods:

- **Right to Ask (R2A)** – where a request for information is made by someone outside of the police. This may be the recipient themselves, or the applicant could be a relative, friend or professional.
- **Right to Know (R2K)** – are entirely generated by police proactively identifying that a potential risk exists.

2.2 The type of entry method must be identified to enable correct NICHE recording, and the fact R2K occurrences generally carry more risk. This is due to the recipient potentially being unaware that a risk exists, which must be a key consideration when managing the process.

2.3 R2A applications will be accepted via online form on the Surrey Police website, through the FCC contact centre and via direct approach to any police officer or staff member with public contact.

2.4 If a police officer or member of staff identifies a potential risk relevant to DVDS/CSODS, they must raise a R2K Niche occurrence.

3. COMPLIANCE WITH LEGISLATION

3.1 All information handling, processing and sharing for DVDS and CSODS must be compliant with the Human Rights Act 1998, the [UK General Data Protection Regulation \(GDPR\)](#) and [Part 3 of the Data Protection Act 2018](#), as outlined in the national guidance.

3.2 The national guidance for DVDS is placed on a statutory footing by section 77 of the [Domestic Abuse Act 2021](#). This means if Surrey Police deviate from the direction of this guidance there must be good reason.

3.3 Surrey Police will comply with the national guidance for both DVDS and CSOD wherever possible. Scenarios or identified risk may justify deviation. Public safety will be the utmost priority above complying with guidance, so long as any proposed action is lawful, proportionate and justified.

3.4 Surrey Police have rationalised 3 specific situations where there will be a general deviation from the DVDS and CSODS national guidance:

1.) Delivery in person - The CSODS national guidance states that both delivery of a disclosure and notification that there is nothing to disclose will be given in person. Surrey police will permit the use of delivery via digital means for CSODS, so long as specific conditions are met (see Method of delivery).

2.) Definition of Serial Perpetrator of DA - The DVDS national guidance uses the Crown Prosecution Service definition of 'where a suspect has committed an act of domestic violence against two or more different victims or complainants, they should be considered a serial perpetrator'. For the purpose of DVDS, Surrey Police will extend this definition to cover two or more incidents involving a single victim or complainant. Allowing researchers to not discount risk that may have occurred in a single relationship.

3.) Decision to disclose – The CSODS guidance states that a disclosure decision will be made by someone of the rank of sergeant or above, whilst the DVDS guidance states that a decision maker will be the rank of inspector or above. In Surrey the decision for both schemes will be made by someone of the rank of inspector or above, or a PSPA sergeant (see Decision to disclose)

All other deviations from the national guidance will be recorded on NICHE along with a rationale.

1. TIMESCALES

4.1 All DVDS and CSODS occurrences must be completed within **28 days**. The only exception to the 28-day limit, is where there are extenuating circumstances.

4.2 Extenuating circumstances are not defined but would need to be something that seriously impacts the ability to either locate the recipient or determine if a disclosure is necessary. For example, attempting to gather information via Interpol from another country where it is likely to be a prolonged process. A plan must be created for dealing with any risk caused by the delay and notifying the recipient/applicant (where appropriate).

For R2A requests specifically:

- Suitable checks must be completed within **24 hours** to identify immediate risk or action required such as breaches of orders, or wanted persons etc. At a minimum this must include a primary review of NICHE and PNC.
- A face-to-face meeting must be held within **10 days** from the occurrence being raised (see face-to-face meeting).

4.3 The force aspiration is that the research element of DVDS and CSOD occurrences will be completed within **14 days**, to allow 14 days to locate the recipient and make delivery arrangements.

4.4 For the purpose of recording timings, a R2A DVDS or CSODS application will be deemed to have started on the day that the request is made. R2K will begin on the day that the potential requirement for disclosure is identified.

4.5 DVDS and CSODS occurrences will be deemed to have concluded on the date that the disclosure is given, is deemed not to be necessary or is made dormant. Where the disclosure is refused the date of conclusion will be the last date that contact was made with the recipient regarding the disclosure.

2. APPLICATION/CREATION STAGE OF THE PROCESS

5.1 Risk assessment

All DVDS and CSODS occurrences will be risk assessed upon first receipt/creation to establish if there is any immediate risk that needs to be addressed and/or any requirement for deployment.

Risk assessments must be recorded on the occurrence OEL. Tools such as the National Decision Model (NDM) and the Authorise Professional Practice (APP) principles of risk must be used where appropriate.

Any risk or requirement for deployment will be dealt with in line with the appropriate policy. For example, the Domestic Abuse Policy if the applicant raises unrecorded DA matters.

If at any stage something is identified that is either high risk or time critical, it must be specifically recorded on the occurrence OEL.

- **High risk** means either a serious or life-threatening issue has been identified. For example, the subject is a registered sex offender and is identified to be living in a

residence with children. However, it may not necessarily relate solely to the risk posed by the subject. It could be due to recipient related issues and vulnerabilities, such as mental health, substance abuse or learning difficulties. Where it is identified that the recipient may not be able to fully understand the risk or have capacity to make decisions to protect themselves.

- **Time critical** means that there is a significant event occurring before the 28-day period has elapsed for completing the application. For example, the people involved are moving in together or are planning on leaving the country together.

The person responsible for identifying the high risk/time critical issue must ensure that it is raised appropriately. A plan must be created to ensure that the matter is progressed appropriately.

The officer/staff designated as officer in case (OIC) will be responsible for ongoing risk assessments.

5.2 Niche Recording and allocation

All applications will be recorded on Niche as stand-alone occurrences. Occurrences must be created as soon as soon as practicable after the request is made (R2A) or the requirement is identified (R2K) and in any case before the end of duty.

Occurrences must be given the correct DVDS/CSODS occurrence type, and the correct NN Stats classification.

All relevant people and addresses must be linked to the occurrence as soon as they are identified. Particular attention must be given to identifying and linking any relevant children.

All occurrences will be tasked on Niche to the Police Single Point of Access (PSPA), regardless of whether or not they are already allocated to the team responsible for their ownership.

PSPA will be responsible for centralised recording, and preliminary data compliance checks.

For occurrences requiring allocation for progression, PSPA will be responsible for allocation to the correct team, based on the following principle:

- If the DVDS or CSODS application relates to a current or recently closed investigation held by a specialist team (non-exhaustive list CID, CAD, DAT, SOIT, POLIT), that team will be responsible for research and disclosure decision making on that occurrence. For all other occurrences, PSPA will be responsible for research and decision making.

DVDS and CSOD occurrences will be managed in the same manner as crime workloads, with general decisions, reviews and direction being made by the OIC and where necessary appropriate supervisors on the responsible team. There are specific rank requirements for disclosure decisions (see Decision to disclose).

All relevant updates must be included on the OEL as soon as possible. At the end of duty, OEL's must be left with a level of detail that would allow an oncoming officer/staff to understand the current situation, risks, and stage of the process (particularly prior to leave or rest days).

Only PSPA will finalise DVDS/CSODS occurrences. All occurrences will be Niche tasked to PSPA when fully complete and ready for filing.

5.3 R2A Face to face meeting

The face-to-face meeting does not necessarily need to be done in person; it can be done via digital technology. The officer/staff responsible must determine which method is best for the applicant.

The face-to-face will be used to gather enough information to aid the research process. A non-exhaustive list would include establishing:

- The identity of the applicant
- The nature of the relationship
- The reason for the application
- What the applicant already knows about the subject's history and any risk posed by them

Sufficient detail must be gathered to ensure that the subject's identity can be confirmed. This may include establishing all given names, aliases, identify document details, and potentially a photograph if available.

If enough information has been gathered during the initial application, then there is no requirement to hold a face-to-face. This is a decision to be justified by the officer/staff responsible.

If something high risk or time critical has been identified, it is acceptable not to delay progressing the application to complete a face-to-face. The officer/staff responsible must still ensure that all necessary prerequisites and data protection requirements are complied with and that subject identity is confirmed.

5.4 DVDS Leaflet

The Surrey Police DVDS leaflet will be given to applicants and recipients, either in digital or printed form.

It will be provided at a suitable point, which for R2A applications should be upon first contact or during the face-to-face. For R2K it should be provided if a disclosure has been authorised, following first contact from police regarding the disclosure.

5.5 Subject in custody

Should a requirement for a DVDS/CSODS become apparent when a subject is in Surrey police custody, all efforts will be made to expedite the process to ensure that a disclosure can be provided while the recipient is in custody.

Consideration must be given to providing an initial threshold disclosure, if it is not possible to provide a full disclosure.

3. RESEARCH STAGE OF PROCESS

6.1 Researcher role

A researcher will be assigned by a supervisor from the team responsible for managing the DVDS or CSODS. They must be suitably experienced and have capacity to complete the research within timeframes (for example, not allocated an occurrence prior to leave).

The researcher may be different from the OIC for the DVDS/CSODS or any related matters. The allocating supervisor must clarify roles and responsibilities.

Research will be completed using the method described in the Operational Guide (Skim Check, Primary Research, 14 Day Review, Secondary Research).

Suitable research must also be carried out into the recipient (and applicant if applicable and necessary), to ensure due diligence around fairness and impartiality, and the balance of risk between the parties, which may impact necessity for disclosure.

The research document and the disclosure document must be used for all occurrences, they must be attached to Niche as soon as they are begun and should be updated as research progresses.

The researcher will be responsible for recording all relevant information in the research document before composing a proposed form of words in the disclosure document.

Researchers must aim to have the research completed within 14 days from when the R2A request was made or when the R2K was raised. A rationale must be provided if this is not achievable. In any case the researcher must be prepared for the 14-day review, being able to explain what research has been carried out, what tasks are remaining, highlighting identified risks, indicating whether a disclosure is likely to be required and whether threshold has potentially been met to disclose.

6.2 14 Day review

By 14 days at the latest, a supervisor from the team responsible for managing the DVDS or CSODS will carry out a review.

The review must consider if threshold has been met, if further research is required and whether any guidance or direction is necessary. Details will be recorded on the occurrence OEL.

6.3 Thresholds

The following threshold will be applied to determine when research should be ceased and disclosure progressed, to ensure that research is carried out to a suitable level to achieve the aim, whilst not being so excessive as to delay disclosures and breach subject rights.

Disclosable information has been and identified AND

It is reasonable to conclude that it fully achieves the aim in a lawful, fair and proportionate manner and that further research or disclosure would not be necessary or proportionate

OR

There is a pressing need to make a disclosure now, to manage risk in a timely manner and comply with the national guidance. Further research and disclosure might be necessary dependent on the outcome of the first disclosure.

The threshold should be continually considered as research progresses. If it is believed that threshold has been met, the matter must be raised for a disclosure decision.

6.4 Types of Disclosure

Surrey Police will recognise three types of disclosure and fourth principle for managing safety.

- **Confirmation disclosure** – The recipient already has enough information about the subject to have an informed view of their character and understands the potential risk they pose. There may be a requirement to clarify or make minor corrections to the information known or disclose some specific risk information (for example the subject stalked previous victims after offending).
- **Initial threshold disclosure** – There is a requirement for an initial disclosure, there may be requirement for further research or disclosure.
- **Full (threshold) disclosure** – Either all available information has been reviewed, or it is believed that the aim has been fully achieved, and no further research is considered necessary or proportionate.
- **Safety check (for R2K or R2A made on behalf on another)** – A risk has been identified that requires contact with the recipient or other confirmation to establish recipient safety, before it is possible to determine if a disclosure is necessary.

The fact that national guidance allows 28 days for a DVDS/CSODS to be completed must not shift focus from managing risk sooner, if necessary, a safety check must be considered.

Safety checks will be used where it is not possible to make an initial threshold decision to disclose the risk known. For example, information exists that a subject may have committed a murder or other serious offence abroad, but it is proving difficult to confirm the information quickly.

Information or updates from reliable sources, such as probation, outreach or social services will be suitable to satisfy the requirements of a safety check, if they mitigate the risk sufficiently.

Safety checks will have careful consideration, rationale and justification to ensure that they do not prejudice the view of the recipient towards the subject or imply that a disclosure will be given prior to a disclosure decision being made.

When a DVDS/CSODS is put forward for a disclosure decision, the type will be recorded, along with any rationale for its use.

6.5 Decision to disclose

The decision as to whether a disclosure is necessary or not will be made by someone of the rank of inspector (or above), or a PSPA sergeant.

They will review both the research document and then the proposed form of words in the disclosure document.

They will direct any required amendments, additions or redactions in the disclosure document.

They will apply the three-stage test, provided in the national guidance and explained in the DVDS and CSOD Operational Guide. In addition, they will give direction on whether the proposed type of disclosure is suitable, who should be disclosed to and how the disclosure should it be made (in person or digitally – see Method of delivery).

All decisions, rationale and any direction will be recorded on the Niche OEL.

4. DELIVERY STAGE OF PROCESS

7.1 Method of delivery

The default position for delivery of DVDS and CSODS will be in person.

To minimise risk and embarrassment to the recipient, in person delivery will be made by officers/staff in plain clothes and unmarked vehicles, unless there is a compelling reason to use uniformed resources.

Digital delivery means the use of video / telephony systems to provide the disclosure to the recipient.

Digital delivery can be used for delivery of both DVDS and CSODS, only if it provides a safer, more expedient, or better service for the recipient, not because it is easier or more convenient for police, and with the following exceptions:

- It will not be used for R2K disclosures, unless there is a compelling reason to do so.
- It will not be used where disclosure is likely to be a significant impact on the recipient (non-exhaustive examples would include – risk of harm or self-harm, disclosure of significant risk offences, or undeclared sex offender, pregnant by subject etc.)

Delivery will be made by video when digital delivery is used, to allow for visual confirmation of identification and assurance that only the recipient or those with a right to hear the information are present.

Telephony will only be used in exceptional circumstances, where video options are not available and there is a compelling need to make the disclosure.

Digital delivery will be made using force approved devices and software.

If digital delivery is used, all identification and data protection prerequisites must still be met. Careful consideration must be given as to how this can be achieved if telephone delivery is being considered.

7.2 Delivery alongside ongoing investigation

When a disclosure is required alongside a relevant investigation, the safety of the recipient will always be the primary consideration.

Where recipient safety can be managed to an acceptable level, an appropriate point will be chosen to make the delivery. There must be consideration given to negating future allegations that the disclosure impacted evidence provided by the recipient. For example a disclosure can be provided following a statement or video recorded interview being provided by the recipient, should it be safe to delay the disclosure.

7.3 DVDS and Outreach

The involvement of Outreach will be considered for all DVDS disclosures, as well as refusals (and non-disclosures when appropriate).

The responsible officer/staff will aim to give advance notice to Outreach to establish if they are able to attend the disclosure either digitally or in person.

Recipients are able to decline consent for outreach to be involved, but high-risk matters will be treated in line with the Domestic Abuse Policy, where consent is not required for the initial introduction.

7.4 Prerequisites prior to delivery

The delivering officer/staff must check and record the form of identification provided by the recipient or explain how identity was confirmed.

If identify cannot be confirmed, there will be no disclosure. The information that was to be disclosed should be considered as intelligence and used for other safeguarding purposes if necessary.

The delivering officer/staff must read the data protection warning (included in the disclosure document) to recipient and ask to them to sign if in the recipient is seen in person.

If using digital delivery methods, or the recipient declines to sign the warning, they must be asked to verbally confirm their agreement. The delivering officer/staff must record this using a suitable method (PNB, INB or BWV etc).

If the recipient refuses to either sign or verbally agree to the warning, the delivering officer/staff must decide as to whether the delivery should progress. If there is likely to be an obvious and preventable data protection breach, a disclosure must not be made.

7.5 Making the delivery

The delivering officer/staff will be responsible for ensuring that the delivery is made in a private space, and that neither the subject nor anyone else without a right to hear the disclosure is present. For digital delivery this may require the recipient to show the delivering officer/staff there is nobody else present.

Disclosures will only be provided verbally. The delivering officer/staff must ensure that they are not being recorded and they must not hand any documents to the recipient or allow copies to be made.

All signed disclosure forms will be scanned and attached to the Niche occurrence, the original must then be disposed of securely. There is no requirement to place documents in and MG6X.

7.6 Refusals

Any refusal must be reviewed by either an inspector or a PSPA sergeant. They will review the reason for the disclosure and provide direction as to whether the refusal should be accepted, whether further attempts should be made, if a different approach should be used, and if there are any other safeguarding actions required.

7.7 Flags and markers

NICHE/PNC flags and markers will be used to highlight that a disclosure exists for the recipient, unless there is a compelling reason not to. For example, there has been good contact with the recipient, and a delivery appointment is already booked.

Disclosures must be authorised for delivery before flags and markers are applied, unless there is a specific reason or identified risk, that requires the recipient to be located. For example, police are willing to tell the recipient that a disclosure is being considered following a request being made on their behalf, but we currently have no method of contacting them.

The wording of any marker used must ensure that it does not place the recipient at risk, for example if they should come to police attention whilst in company with the subject.

The marker types used will be 'locate trace' for PNC and 'BOLO' for NICHE.

5. SAFEGUARDING AND REFERRALS

8.1 Safety plans

Following delivery of a disclosure, the delivering officer/staff will have a discussion with the recipient, to establish their response to the disclosure, their intentions and any other support required.

Where necessary, the delivering officer/staff will complete a safety plan based on this discussion, details of which should be recorded on the OEL.

Any action related to the safety plan must be raised and progressed as appropriate.

Safety plans will be considered throughout the process, as there may be occasions where they are required prior to a disclosure or following a decision not to disclose or a refusal.

8.2 Support services

The delivering officer/staff must be prepared to signpost the recipient towards support services, as outlined in the national guidance and the operational guide.

Support services for the perpetrator must also be considered.

8.3 Signs

A Signs adult/child at risk (as appropriate) will be completed for every disclosure that is given or refused, in line with the Signs Adult Policy and Signs Child Policy.

Signs must be completed as soon possible after the disclosure/refusal and in any case prior to the end of duty.

The Signs will include details of all relevant adults and children.

The Signs must not include a full copy of the disclosure given to the recipient, but it must include an indication of what was disclosed. For example, 'DA in the current relationship and sexual assaults'.

The Signs must include sufficient information to ensure social services understand the risk and issues, to aid their decision making. A non-exhaustive list of information to include would be how the recipient responded to the disclosure, what their intentions are, whether they intend to cease the relationship/contact.

8.4 3x5x2 Intelligence report

A 3x5x2 intelligence report will be completed for every disclosure that is given or refused, to allow the notification to be automatically uploaded onto the Police National Database (PND).

The intelligence report must be completed as soon possible after the disclosure/refusal and in any case prior to the end of duty.

The detail in the intelligence report will only state that a disclosure was given or refused and referencing the relevant Niche occurrence number.

8.5 Offender management

Subjects identified through DVDS/CSODS enquiries will be considered for suitable offender management schemes when appropriate. High-harm perpetrator units will provide advice on requirements and actions.