



Home Office

The Child Sex Offender Disclosure Scheme (CSODS)

Police Guidance

April 2023

Contents

1. Introduction.....	3
2. What is the Child Sex Offender Disclosure Scheme?.....	4
Figure 1: Overview of Child Sex Offender Disclosure Scheme entry routes	5
3. The Process	6
3.1 The “Right to Ask” entry route	7
Step 1 – Initial contact with police	7
Step 2 – Follow up investigation and contact with the applicant.....	9
Step 3 – Full risk assessment	11
3.3 Applicants under 18 years.....	12
3.4 Subjects under 18 years	13
3.5 Cross border applications	13
3.6 Referral to a local multi-agency public protection arrangements meeting	14
3.7 Categorising a “concern” or “no concern”.....	15
3.8 Disclosure decision-making process	16
Principle 1: Three-stage disclosure test.....	17
Principle 2: Data Protection Act 2018	17
Principle 3: Informing the subject of the disclosure	17
Decision made to disclose information.....	18
3.9 Maintaining a record of the Disclosure Scheme	20
3.10 Timelines.....	21
4. Definitions used within the scheme	22

1. Introduction

- 1) Child sexual abuse is an horrific crime that has a devastating impact on victims' lives. In 2021, the Centre of Expertise on Child Sexual Abuse estimated that at least 15% of girls and 5% of boys experience some form of sexual abuse before the age of 16.¹
- 2) The Child Sex Offender Disclosure Scheme (CSODS) is often known as "Sarah's Law" after Sarah Payne, the victim of a high-profile murder in 2000. The principle aim of this scheme is to provide parents, guardians, and carers with information that will enable them to better safeguard their children's safety and welfare. It introduced the principle of a two-way disclosure by enabling the public to ask about the history of a person who has access to their child. The scheme was rolled out nationally in 2011 after working with Sarah's parents to enable limited public access to information about registered sex offenders, often referred to as the "sex offenders' register".
- 3) The CSODS was not based on any new legislation, but it provides structures and processes for the exercise of existing powers. Any disclosure must be within the existing legal framework and have due regard to the established case law, the Human Rights Act 1998, and the UK General Data Protection Regulation and Part 3 of the Data Protection Act 2018.
- 4) The purpose of this guidance is to support the delivery of the CSODS and inform those involved in the application process.
- 5) It is important to remember that the purpose of this scheme is to protect children from harm. Each request for information will be dealt with on a case-by-case basis and, while there may not be information that can be disclosed in accordance with the CSODS, disclosure of other relevant information may still be possible.
- 6) Definitions of terms used in this guidance are included at the end of the document.

¹ Karsna, K., Kelly, L (2021). 'The scale and nature of child sexual abuse: Review of evidence'. Available at: <https://www.csacentre.org.uk/documents/scale-nature-review-evidence-0621/>.

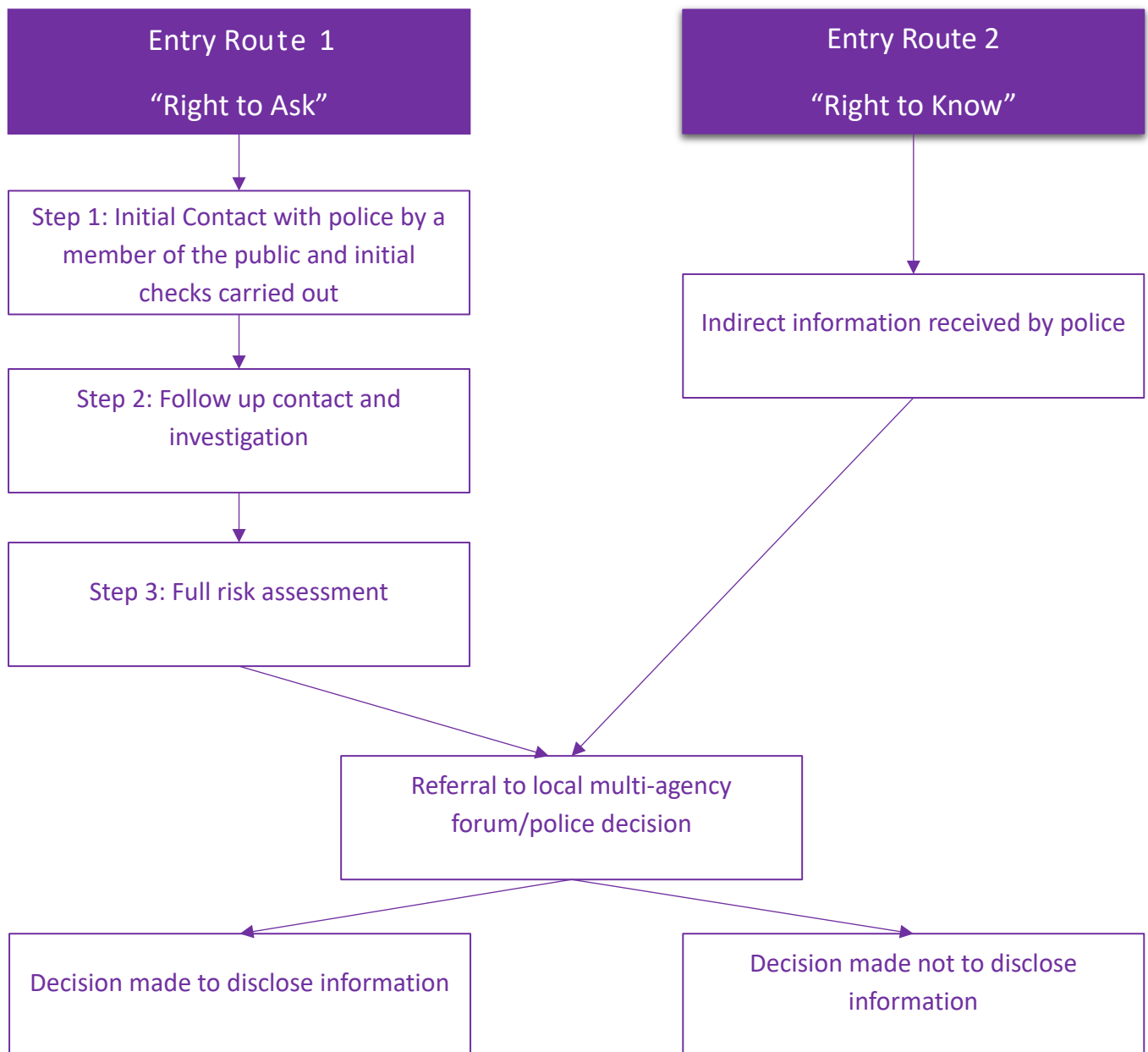
2. What is the Child Sex Offender Disclosure Scheme?

- 7) The Child Sex Offender Disclosure Scheme (CSODS) is not the result of new legislation; rather, it builds on existing law and procedures and provides a clear access route for the public to raise child protection concerns.
 - a) [The Multi-Agency Public Protection Arrangements \(MAPPA\) Guidance](#) is statutory guidance under Section 325 (8) of the Criminal Justice Act 2003 and it explains how responsible authorities should approach the issue of disclosure.
 - b) [Section 327A of the Criminal Justice Act 2003](#) places a duty on each MAPPA authority in every case managed by it concerning a convicted child sex offender to consider disclosure to particular members of the public.
 - c) [The Working Together to Safeguard Children Statutory Guidance](#) on inter-agency working to safeguard and promote the welfare of children.
 - d) [Social Services & Wellbeing \(Wales\) Act 2014](#) & [Working Together to Safeguard People \(Wales\) 2015](#)
- 8) The CSODS recognises two procedures for disclosing information (processes for which are presented at [Figure 1](#)):
 - a. “**Right to Ask**” is triggered by a member of the public applying to the police for a disclosure.
 - b. “**Right to Know**” is triggered by the police making a proactive decision to protect a potential victim.
- 9) It is important for all involved to remember that, in delivering this scheme, potential or actual victims of child sexual abuse are protected from harm. By making a request for disclosure, a person will often be registering their concerns about possible risks to children they know. For that reason, it is essential that this scheme is not used in isolation. Critically, police forces should work closely with partners through the Multi-Agency Public Protection Arrangements (MAPPA) where needed and have consideration of other safeguarding issues to ensure that any possible risk of harm to children are fully assessed and managed.
- 10) The CSODS is focused on disclosure and risk-management where the subject is identified as being convicted (including cautions, reprimands, and final warnings) of child sexual offences. **For the purposes of the scheme, a child sexual offence will be defined as any offence listed under [Schedule 34A of the Criminal Justice Act 2003](#).**
- 11) The CSODS may overlap with and complement other disclosure processes, such as MAPPA, Multi-Agency Risk Assessment Conference (for the risk of reducing domestic violence) or the Domestic Violence Disclosure Scheme (DVDS - sometimes known as “Clare’s Law”). Consideration should be given to which process is the most appropriate in each case. Forces should aim to make the process of applying to both schemes as easy as possible, and **applicants should not be asked to provide their information separately for each scheme**. Forces should ensure that, where an application is made for a single scheme (either CSODS or DVDS), they consider a disclosure of information under “Right to Know” for the other scheme without the need for the applicant to make a separate application.
- 12) The CSODS does not replace statutory child protection procedures and, if a current risk to a child is identified that requires more than simply disclosure being considered, the case

should be transferred into a Multi-Agency Safeguarding Hub for progression and consideration.

- 13) The CSODS does not replace existing arrangements for Disclosure and Barring Service (DBS) checks, Subject Access requests or Freedom of Information (FOI) requests.

Figure 1: Overview of Child Sex Offender Disclosure Scheme entry routes



If it is identified that urgent action is required due to immediate/imminent risk of harm to a child, then **RING 999 IMMEDIATELY**.

Note: a decision not to proceed with a disclosure, based on an appropriate assessment of risk, may be made at any stage of the process.

3. The Process

- 14) Under the CSODS, anyone can make an application about a person (subject) who has some form of contact with a named child or children. This could include any third party, such as a grandparent, neighbour, or friend.
- 15) In the event that a subject has convictions for sexual offences against children, poses a risk of causing harm to the child concerned, and disclosure is **necessary** to protect the child and is a **proportionate** response to manage that risk, there is a presumption that this information will be disclosed. However, it is important to note that **any disclosure under CSODS will only be made to the person best placed to protect the child**. This may not be the individual that made the application.
- 16) It should be noted that the presumption to disclose will only exist in cases where the subject has convictions for child sexual offences. However, it is important to recognise that many sexual offences against children are committed by persons who are not current or archived Registered Sex Offenders.
- 17) Equally important is the fact that there are often links between sexual and violent offending, and this type of offending should not be ignored. Likewise, information may be held about the subject of the CSODS application which may not be convicted offending, but still demonstrates that that subject may pose a risk of harm to the named child or children.
- 18) In terms of other relevant information held by the police about subjects who do not have convictions for child sexual offences, an examination of the provenance, reliability and credibility of that information must be completed prior to any disclosure being authorised. Subjects who do not have convictions for sexual offences against children but may still pose a safeguarding risk to the named child or children could include (but are not limited to):
 - a. Persons who are convicted of other offences, for example serious domestic violence or child cruelty/neglect.
 - b. Persons who have not been convicted but on whom the police or any other agency holds intelligence or other information indicating that they pose a risk of harm to children.
- 19) The CSODS is a gateway to allow the public to raise concerns about individuals who may pose a risk to children. Therefore, while information that is not a conviction for a child sexual offence is not covered by the presumption to disclose as set out within [Section 327A of the Criminal Justice Act 2003](#), disclosures should be considered on a case by case basis when such information is held. This is to ensure that appropriate action is taken to protect children wherever possible.

3.1 The “Right to Ask” entry route

Step 1 – Initial contact with police

- 20) An application will be considered to have been made when a member of the public contacts the police to ask for information about whether a person poses a risk of sexual harm to a named child or children. Initial contact can take place via online application forms, over the phone, or in person at a police station.
- 21) For the purposes of this guidance: “the subject” is the person about whom a CSODS request is made, “the applicant” is the person making the request for information, and “the recipient” is the person receiving the disclosure (if different from the applicant).
- 22) If at any stage during the CSODS application process the police believe that a crime is being alleged, they will pursue the crime report under normal investigation and recording procedures. However, it is possible, on some occasions, for a CSODS application to run concurrently with a criminal investigation, but a formal strategy should be agreed with the team investigating the criminal matter about how to best progress the CSODS application to ensure that there is no compromise to the criminal investigation. It may be determined that the issue of safeguarding and disclosure may be better placed to be progressed as part of the criminal investigation.
- 23) If a request for information is made to a partner agency rather than the police, the normal procedures adopted by the partner agency for handling this type of request will apply. Disclosure of information is not a safeguarding tool available only to the police; other agencies may have disclosure powers and should act according to their own safeguarding frameworks. However, if the applicant makes it known that they are making an enquiry under CSODS, then they should be referred to the police. A partner agency may facilitate contact with the police if it is appropriate.
- 24) However, if the CSODS applicant has already received disclosure via an alternative mechanism (for example via a MAPPA level 2 or 3 meeting or a safeguarding strategy discussion) but are requesting further information or clarification about that original disclosure, the applicant should be redirected to the agency or team that was responsible for that original disclosure decision rather than create a separate enquiry under CSODS. This avoids duplication of processes and ensures a continuity of oversight for the case.
- 25) If the child is subject to open child protection procedures, agencies should utilise the provisions within those frameworks to consider disclosure as part of their safeguarding plan, rather than direct a separate application for CSODS. This is to avoid the applicant having to go through an alternative process and having to engage with other professionals when the agencies involved in the child protection procedures can deal with such matters proactively themselves.
- 26) If the applicant visits the police station in person, they must be allowed the opportunity to make their enquiry in private, as they may feel uncomfortable doing so in the hearing of other members of the public.

NOTE: It is vital that, at this stage, a safe means of communication is agreed where the place, means and timing is determined by the applicant. This is critical to safeguarding the applicant.

Information to be obtained and communicated during the Initial contact

- 27) After receiving the initial contact, the police officer / staff member must take all the details from the applicant and complete an Initial Contact and Face-to-Face Form (Annex A). Initial contact can take place via online application forms, over the phone, or in person at a police station.
- 28) During the initial contact stage, police will also remind/inform the applicant of the following:
- a) The CSODS does not replace existing procedures that are in place for subject access or Freedom of Information (FOI) requests and the Disclosure and Barring Service (DBS).
 - b) A disclosure will only be made to the person who is in the best position to protect the child or children named in the enquiry.
 - c) The need for disclosure is based on the risk posed by the subject to the named child and will depend on the level of contact that the subject has with the child or children.
 - d) Initial checks will be completed as soon as possible and in any case within 24 hours. These checks will assess whether there is an immediate or imminent risk of harm to the child or children named in the application, which means the subject may present a risk before the minimum checks are undertaken. They will also assess whether the disclosure application should be progressed further.
 - e) Should a decision be made to progress the disclosure application further:
 - i. The disclosure will be referred to the police's appropriately trained staff to deal with; and
 - ii. The applicant will be required to attend a face-to-face meeting within the next 10 days if required. In some circumstances, the police may decide to conduct the follow up contact by telephone or alternative means. At this point, the applicant will be required to provide proof of their identity.
 - f) The police will aim to complete the follow up contact within 10 days, but there may be extenuating circumstances that increase this timescale. The applicant will be informed if this is the case.
 - g) If any immediate risks are identified at any stage, immediate safeguarding action will be taken. A safety plan will also be developed if a disclosure takes place.
 - h) Further information on the scheme is available in the Public Guidance for the scheme. Information on how to spot the signs of abuse and keep children safe is available in the Keeping Children Safe from Sexual Abuse Guidance.

Initial intelligence research to be completed

- 29) Once the initial contact form has been completed by the receiving officer / police staff member, the form must be submitted to the appropriate police team to conduct research on the named party. Checks should focus on the risk posed by the subject but have due regard to known concerns about the child or children named; for example, if they are subject to current child protection procedures. **Given that the application is potentially raising concerns about a named child, the police must be able to undertake such checks on a 24/7 basis to ensure any immediate risks can be identified and managed effectively.**

- 30) If immediate concerns are identified during the initial checks and research enquiries, appropriate action must be taken to safeguard those at risk. The officer responsible for the research and enquiries must report the concerns to a supervisor immediately.
- 31) **A maximum timescale to complete the initial checks following the applicant's initial contact with police will be no more than 24 hours.**
- 32) If no immediate concerns are identified during the initial checks and research stage, the application and checks will be forwarded to the team that are responsible for investigation and progressing the case.

Step 2 – Follow up investigation and contact with the applicant

Decision on whether to progress Disclosure Application

- 33) Once the case has been sent to the responsible team, in accordance with the local police procedures, it will be for the police to:
 - a. Decide whether to progress the application following the initial risk assessment; and
 - b. Determine how the applicant will be contacted to progress the disclosure application consistent with the preferred method agreed at initial contact.
- 34) The case must be reviewed and supervised by an officer of at least the rank of Sergeant or Police Staff equivalent, who has knowledge of the scheme and is experienced in dealing with safeguarding and the risk management of offenders.
- 35) At this stage, a formal report needs to be created on the force case/crime management system (creating a reference number) to ensure there is an auditable record of the CSODS application being made.

Follow up investigation and contact with the applicant

- 36) If the police decide that the application should continue, the applicant should normally be seen in a face-to-face meeting. This should take place as soon as possible and, in any event, **no later than 10 working days after initial contact**. This is to:
 - a. Ensure the request is genuine and not malicious;
 - b. Establish further details about the application in order to further assess risk and to inform decision around disclosure;
 - c. Provide safety information and advice to safeguard the child in question; and
 - d. Ensure that there is an opportunity to explore potential wider safeguarding issues, in addition to the potential issue of the disclosure of information. This could include the lived experience of the named child and the exploration of contact with other persons not named in the initial application.
- 37) The face-to-face contact should be conducted by an officer or police staff member who has received in-force training to ensure they have a baseline understanding of child safeguarding and the risks posed by sex offenders. Experience in these areas will assist in relevant questioning and the identification of behaviours that will inform any subsequent risk assessment.

- 38) It may be appropriate for this stage of the application to be followed up by way of a telephone/video call interview rather than face-to-face contact. This will be considered on a case-by-case basis and is most suitable when full checks have been completed and it is found that there is no information held that identifies the subject as a potential risk to children. If the applicant is raising concerns about the behaviour of the subject which suggests that there is an ongoing concern, even when no other information is held about the subject, then face-to-face contact is recommended for further exploration of such concerns.
- 39) The option to undertake the interview in a neutral location should be provided, but it is best practice to conduct a face-to-face contact at the home address of the applicant when the applicant resides with the named child/children.

Preliminaries

- 40) Before progressing enquiries on the application, the police must:
- a. Warn the applicant that, if they wilfully or maliciously provide false information to the police in order to try to get a disclosure to which they are not entitled, they may risk prosecution.
 - b. Warn the applicant that, if they disclose evidence of an offence whilst registering a concern, it may not be possible to maintain their confidentiality.
 - c. Warn the applicant that information disclosed by the police must only be used for the purpose for which it has been shared.
 - d. Assure the applicant that the application will be dealt with confidentially. However, this can only be guaranteed pending the outcome of the process. In the event of a concern arising about the subject, the police must consider whether representations should be sought from the subject. Moreover, if a resultant disclosure is to be made, the police must consider if the subject should be told about the disclosure.
 - e. The applicant will be asked for proof of identity, either in person or online. Acceptable forms of ID may include:
 - (i) Passport;
 - (ii) Driving licence;
 - (iii) Other trusted form of photo ID;
 - (iv) Household utility bill (electricity, council tax, gas, water);
 - (v) Bank statement.
- 41) If the applicant does not have any of the above forms of ID, this will not necessarily prevent an application. It may be possible to refer to another agency to confirm the applicant's identity (e.g. social worker, health visitor).
- 42) **A disclosure cannot be made without verification of identity or if the applicant chooses to remain anonymous.** However, if either of these two eventualities arise, checks will still need to be made on the information given about the subject and, if concerns are identified, appropriate measures will still need to be taken.

During the face-to-face meeting

- 43) The face-to-face meeting should be approached with an investigative mind-set, not simply to resolve the issue of potential disclosure but to fully consider the wider safeguarding situation of the named parties.
- 44) During the face-to-face meeting, the applicant will be asked what they already know about the subject's history. It may be the case that they have information from other sources (for example, the media) that is accurate and sufficient for the purpose of the applicant being able to protect the child, thus negating the need for further disclosure. Alternatively, they may have been given information (for example, from the subject themselves) that is inaccurate and misleading, and disclosure may be required to ensure the applicant is fully aware of the risks, despite that previous information being available to them.
- 45) If initial searches have not uncovered any pertinent information relating to the subject, the applicant should be asked to provide additional information that will enable the correct identification of the subject. This may include a photo or a description of identifying features such as tattoos and birthmarks, as well as details of previous addresses and places of work.
- 46) The applicant will be informed that, if a disclosure is authorised, the person to whom the disclosure is made will be asked to sign an undertaking that they agree that the information is confidential and they will not disclose the information further. Legal proceedings could result if this confidentiality is breached, for example under [Section 170 of the Data Protection Act 2018](#). If the recipient is not willing to sign the undertaking, the police will need to consider if disclosure should still take place.
- 47) If the police are made aware that the subject has access to children other than the one(s) named in the application, they must consider whether further disclosures should be made under existing provisions. **It is not for the person receiving the disclosure to share the information received any further.**
- 48) After the face-to-face meeting, the applicant should be provided with information on how to protect children from child sexual abuse (Annex F). This can be provided in leaflet form or via a link to online resources.
- 49) **No decision will be taken at the end of the face-to-face meeting** (unless an urgent safeguarding children enquiry has been initiated due to the risk assessment and some form of disclosure is unavoidable to deal with this). The full risk assessment needs to be undertaken first.
- 50) At the conclusion of the face-to-face meeting, the officer / police staff member will complete the Initial Contact and Face-to-Face form (Annex A) which records the full details of the contact and provides recommendations for next steps that are required. This information is to be sent back to the team responsible for the overarching coordination of the application and investigation. The information must be saved onto the case/crime management system.

Step 3 – Full risk assessment

- 51) Following the face-to-face meeting, the police team responsible for the coordination of the application will conduct a further risk assessment. This will include a revisiting of information

already obtained, checking all available systems, and ensuring that the subject has been correctly identified.

52) Checks will also be completed with other agencies where appropriate. This will include:

- a. Social services (where the applicant has given consent or where the circumstances of the enquiry dictate that this is necessary without consent);
- b. Probation service; and
- c. Any other agency that can provide information to inform the risk assessment.

3.2 The “Right to Know” entry route

53) The “Right to Know” entry route to the CSODS is where the police receive indirect information that may impact the safety of children and which has not been conveyed through the “Right to Ask” process. This could include (but is not limited to):

- a. Information becoming known to the police about a relationship involving a child sex offender and a person who has responsibility for a child or children.
- b. Information obtained during an investigation into other matters that identifies a need for a person to receive information about someone who may pose a risk to a child.
- c. Information received that suggests impending contact between a named child and a person who poses a risk to them.

54) The purpose of the “Right to Know” entry route is to allow the police to act proactively when they are in receipt of information about a risk to a child or children, rather than directing the individual to have to make an additional request to the police when it is already known that disclosure is necessary and proportionate.

55) The “Right to Know” entry route to CSODS does not replace statutory safeguarding processes in place and relevant referrals will still need to be made as required.

56) To ensure that the safeguarding response is proportionate and in line with the risks identified, the police may prioritise which potential disclosures receive a full risk assessment.

57) If a “Right to Know” scenario is identified, then the case should be referred into the team that oversees and coordinates CSODS applications for the circumstances to be assessed.

3.3 Applicants under 18 years

58) If the applicant is aged under 18 years of age at the time of their application, they will be required to be accompanied by a responsible adult when attending the face-to-face follow up meeting stage of the application. If it is deemed appropriate to make a disclosure to a person under 18, the disclosure should also be made to the named responsible adult. The responsible adult could be a family member, a friend, or a professional such as a teacher or social worker.

- 59) Under exceptional circumstances, an application made by an individual that is under the age of 18 who does not have a family member, friend or professional to accompany them can be progressed if no responsible adult can be identified. Consideration should be given to alerting social services to inform them of the details of the application and any subsequent disclosure.

3.4 Subjects under 18 years

- 60) Offending that occurred when the subject was under 18 years of age should be considered by the police for disclosure if it is relevant and timely to the safeguarding of a child. Due consideration should be given to the nature of the offending, including factors such as: the ages of the parties; the emotional maturity of the parties; any coercion or corruption; and the relationship between the parties, including whether there was any existence of a duty of care or breach of trust.
- 61) If the subject of an application is under 18 years of age and there is nothing to disclose, the application should be treated as a normal CSODS application but, depending on the details of the case, consideration should be given to alerting social services to inform them of the details of the application.
- 62) If the subject of an application is under 18 years of age and there is something to disclose, Principle 3 of the decision-making process will apply, as set out in [paragraph 87](#). In the event that the subject is to be informed of the disclosure, this should be done so in an age-appropriate manner, with consideration given to informing their parent, guardian, or carer. Due consideration should be given to the impacts that a disclosure may have on a subject under 18 years of age, and subsequent safeguarding and wellbeing needs must be considered by all relevant professionals involved in the subject's life, including the police. Social services and (where applicable) the offender manager should also be involved in discussions to work with the subject to change behaviours.
- 63) If the subject of an application was under 18 years of age when they committed a relevant offence but is now over 18, the handling of the application will depend on the circumstances and should be managed by police and MAPPA bodies in the normal way.

3.5 Cross border applications

- 64) There is a possibility that there will be applications that require the involvement of more than one Police Force. In these scenarios, it is imperative that there are clear lines of communication between each force to ensure all enquiries are completed.
- 65) **Coordinating Force** – The police area where the applicant resides will be the force that will be responsible for recording the application, conducting the risk assessment, and coordinating the relevant enquiries. This force will be required to complete the follow up contact.
- 66) **Responding Force** – The force area in which any party other than the applicant lives. These forces will take responsibility for actions in relation to these parties (i.e. the subject, the child/children). It will be necessary for the Responding Force to report back to the Coordinating Force with their findings and within agreed timescales.

- 67) All Police Forces and agencies should work in close consultation to consider and address the risk posed in each case. Every effort should be made to reach an agreement between all force areas and agencies involved. In most circumstances, the Coordinating Force will determine whether a disclosure under CSODS is required as they will own the investigation. When the subject is an offender currently subject to offender management by another force, it is recommended practice that the decision about disclosure is jointly reached between both Coordinating Force and the force responsible for the ongoing management of the offender. In the unlikely event that an agreement cannot be reached between all parties about the issue of disclosure, the responsibility for the final decision on disclosure will depend on whether or not the subject is a current MAPPA subject.
- a. In the event that the subject is a current MAPPA subject, the MAPPA area responsible for that subject will have primacy as they have the responsibility of minimising the risk associated with that subject, including the risk of offending against the named child(ren). This police force will duly consider whether a referral is required into level 2 or 3. The police force is able to make a decision on disclosure under their own procedures if level 2 or 3 is not necessary.
 - b. In the event that the subject is not a current MAPPA subject, the force with responsibility for the children will have primacy as they hold the responsibility for the welfare of those children in their area. They will then host the decision-making process for disclosure, determining whether it requires single- or multi-agency involvement.
- 68) Enquiries and referrals (as required) must be made with the agencies in all relevant areas, particularly with the Children's Social Care departments for where the children reside.

3.6 Referral to a local multi-agency public protection arrangements meeting

- 69) If the case relates to a MAPPA eligible offender, consideration should be given as to whether it is necessary to make a referral into a level 2 or level 3 having due regard to the circumstances of the case and the information gathered. Referrals into level 2 or 3 for eligible offenders are the responsibility of the Lead Agency, which is often not the police. Therefore, there needs to be engagement with the Lead Agency when CSODS applications are made about current MAPPA offenders so they can consider what steps they wish to take.
- 70) For a decision to be made simply on whether third party disclosure is required, level 2 or 3 conferencing for a case may not be required, and the decision can be made in accordance with local agency procedures. The MAPPA [guidance](#) provides further information on disclosure decisions for nominals currently within the MAPPA process.
- 71) If the police are the owners of the information that is to be disclosed, they have the ability to authorise disclosures for a statutory purpose without the need to seek authority from other agencies. If other agencies are involved in the case, then it is best practice to consult with them during the investigation and to consider any representations that they may wish to make with regards to the issue of disclosure.

72) At this point in the disclosure scheme process, it is envisaged that the police will have sufficient information to determine whether a credible risk of harm to a child exists. The police should categorise the information as either representing a “concern” or “no concern”. There may be occasions where the police feel it is necessary to refer the case to a MAPPA meeting before a decision is made. This is at the discretion of the individual police force.

3.7 Categorising a “concern” or “no concern”

73) The application will be one raising “concerns” where:

- a. The subject has convictions for child sexual offences as listed under Schedule 34A to the Criminal Justice Act 2003;
- b. The subject has other convictions relevant to safeguarding children (e.g. adult sexual offences, violence, drugs or domestic abuse);
- c. There is intelligence known about the subject relevant to safeguarding children (e.g. cases not proceeded with or intelligence concerning sexual or violent offences, or previous concerning behaviour towards children); and/or
- d. There is concerning behaviour relevant to safeguarding children now being displayed by the subject or child that has been disclosed as part of the disclosure application (e.g. grooming or changes in behaviour that indicate sexual harm to children might be likely or sexual harm may have occurred).

74) There will need to be an identifiable line of risk between the subject and the named child or children to categorise the case as one of “concern”. If there is no contact between the subject and the named child, nor is there sufficient likelihood of contact between the subject and the named child in the future, the case may fall into the “no concern” category.

75) The application will be one raising “**no concerns**” where:

- a. The subject has no convictions that raise child safeguarding concerns;
- b. There is no other intelligence held by police that would indicate that the subject raises child safeguarding concerns; and
- c. The application has not revealed any concerning behaviour relevant to safeguarding children or the application has not revealed any connection between the subject and the named children that would justify disclosure.

76) It is important to stress to the applicant that safeguarding children is a continual process and, even where a disclosure has not been made, it does not necessarily mean that there is no risk of harm to the child and the applicant should therefore continue to take steps to safeguard the child using the advice provided. The applicant/recipient will be given information to empower them to safeguard the child in the future. It will also involve giving

advice on what to do in the event of future concerns and providing general safeguarding children advice.

- 77) This stage of the process should be reached no later than 28 days from the initial contact checks (under “Right to Ask”) or from receipt of the indirect information (under “Right to Know”).
- 78) The Sergeant / Police Staff equivalent who is responsible for the supervision of the CSODS investigation will categorise whether the case is one of “concern” or “no concern”. If the case is one that is categorised as of “concern” and one of the outcomes required will be disclosure of information about the subject to the applicant or other appropriate person, the decision-maker will follow the steps detailed in the disclosure decision-making process section and seek the appropriate authority required to disclose. The decision-maker must, in all cases, ensure that all safeguarding issues that have been identified are addressed.
- 79) If there is no contact between the subject and the named child, nor is there sufficient likelihood of contact between the subject and the named child in the future, the applicant should be informed that their application does not meet the requirements of the scheme and will not be progressed. The applicant should be provided with the Keeping Children Safe from Sexual Abuse guidance (Annex F) and assured that any safeguarding concerns highlighted during the application process will be addressed.

If it is identified that there is an immediate/imminent risk of harm to a child, then action must be taken by the police immediately to safeguard those at risk.

3.8 Disclosure decision-making process

- 80) There must be sufficient access to or connection with the child by the subject to pose a real risk of harm and therefore justify disclosure. This contact does not necessarily need to be for a prolonged period of time as abuse can happen in a relatively short space of time.
- 81) When considering disclosure, it is important to understand what the intended recipient already knows about the subject’s offending/risk history and whether they already have sufficient information to be able to act protectively towards the named child. If they have factually accurate information about the subject, it may negate the need for further disclosure. Alternatively, if the information they do have is not enough to be able to protect the child, then it may be determined that more information should be disclosed.
- 82) There is a general presumption that details about a person’s previous convictions are confidential. There are therefore three principles that the police will need to consider before deciding to disclose information.

Principle 1: Three-stage disclosure test

83) The police have the common law power to disclose information about an individual where it is necessary to do so to protect another individual from harm. The following three stage test will need to be satisfied before a decision to disclose is made:

- a. It is reasonable to conclude that such disclosure is necessary to protect a child from being the victim of a crime;
- b. There is a pressing need for such a disclosure; and
- c. Interfering with the rights of the subject, including their rights under Article 8 of the European Convention on Human Rights, is **necessary and proportionate** for the prevention of crime. This stage of the test involves considering:
 - i. Whether the subject should be asked if they wish to make representations to ensure that the police have all the necessary information at their disposal to conduct the balancing exercise; and
 - ii. The extent of the information that needs to be disclosed. For example, it may not be necessary to tell the applicant the precise details of the offence for the recipient to take steps to protect a child. Disclosures should be limited to only that information that is necessary to protect a child from harm.

84) There may be concerns that relate to the subject's current behaviour towards a child within the disclosure application, for example sexually inappropriate behaviour or grooming. In this case, even though there is no recorded information held by the police or other agencies to disclose to the applicant, they must still be contacted to talk about concerns over the subject's current behaviour. **The CSODS is not simply about whether disclosure of information is required; it is a gateway to allow safeguarding concerns to be raised to the police which will need to be investigated accordingly.**

85) The decision-maker must, in all cases, ensure that all safeguarding issues that have been identified are addressed, and consider the use of additional tools that may be available to manage the risk of harm. This could include the application for a Sexual Harm Prevention Order or Sexual Risk Order, referrals into either the MAPPA or Potentially Dangerous Persons processes, or a referral into a Multi-Agency Risk Assessment Conference (MARAC).

Principle 2: Data Protection Act 2018

86) Information considered for disclosure may include sensitive, personal data (such as information about a person's previous convictions). Therefore, the police must also be satisfied that disclosure is in accordance with the Data Protection Act 2018.

Principle 3: Informing the subject of the disclosure

87) Consideration must be given to seeking representations from the offender before a decision is made to disclose, in order to ensure that all of the information necessary to make a properly informed decision is available. The subject may wish to be involved in the

disclosure process, by way of self-disclosure, and the decision-maker will need to consider whether that would be a safe option.

- 88) Seeking their representations should be the norm, but there might be occasions when it is not possible or safe to do so. These might include, but will not be limited to, those where involving the subject would:
- a. Risk prejudicing an ongoing or prospective criminal investigation;
 - b. Give rise to or increase the risk of harm to children or the applicant;
 - c. Give rise to or increase the risk of harm to a new partner;
 - d. Risk reinforcing grievance-thinking on the part of the subject in a way that would increase the risk presented by them generally;
 - e. Mean disclosing information of which the subject is not aware, and informing the subject would risk compromising intelligence sources or putting such sources at risk;
 - f. Delay the process where disclosure is necessary to avoid an imminent risk of harm and therefore there is not enough time to seek representations; or
 - g. Not be possible as the subject cannot be traced.
- 89) If the subject is to be informed that a disclosure will be made to the applicant or recipient, the subject must be told in person, given information about the CSODS, and be told about the possible implications for them.
- 90) As part of any decision-making relating to the disclosure, an assessment of the impact of the disclosure on the subject must be made. The assessment must include whether the subject themselves may be exposed to any risks, and measures taken to mitigate such risks if they exist. An assessment must be made on whether the recipient is a suitable person to receive the disclosure to ensure that the disclosure itself does not create more risks than it safeguards against.

Decision made to disclose information

- 91) It is recommended best practice that the decision on whether disclosure is authorised is made by an officer of at least the rank of Police/Detective Inspector or Police Staff equivalent. Decision-making by this rank of officer will ensure that the decision is made at a senior enough level and allow for there to be appropriate detachment from the operational management of the subject for the CSODS application to be considered with an appropriate degree of independence. The oversight of this rank of officer is only required when authority to disclose information to a third party is sought by the supervising Sergeant / Police Staff equivalent. If there is no need for disclosure to be considered, the Sergeant / Police Staff equivalent with knowledge of the scheme will finalise the case accordingly.
- 92) If the decision is made to disclose information because it is judged that there is a risk of harm to a child that warrants a disclosure, then the following considerations should be made:

a. What will be disclosed?

A form of specific wording will need to be authorised by the decision-maker and recorded on the case management system. The wording must be sufficient to allow the recipient to understand the risks and then be able to use the information to safeguard the child/children. The wording authorised must be no more than is necessary to achieve this aim. Vague or ambiguous wording can lead to the recipient being left confused about the risk and unsure on what to do next; therefore, the wording must be clear and concise. The disclosure of information should be accompanied by details of how the recipient can and cannot use the disclosure, along with what other support provisions are available.

b. Who should the disclosure be made to?

The disclosure should be made to the person or people best placed to safeguard the child. Whilst many disclosures are made to the applicant, it may not be appropriate to do so in all circumstances.

c. How will the disclosure be made?

The disclosure will be delivered by the police; however, other agencies may be present. The disclosure will always be made in person and will take place at a safe time and location.

93) If a disclosure is to be made, then the person receiving the disclosure will receive the following information:

- a. The disclosure must only be used for the purpose for which it has been shared i.e. to safeguard the child or children.
- b. The person to whom the disclosure is to be made will be asked to sign an undertaking that they agree that the information is confidential and they will not disclose the information further.
- c. Legal proceedings could result if this confidentiality is breached, which should be explained to the person before they sign the undertaking.
- d. If the person receiving the disclosure believes that further children are at risk and further disclosure is required to safeguard them, they should talk to the police who will then make a decision about whether the information needs to be disclosed to others. It should be explained that the recipient should neither make that decision nor make any further disclosure themselves.
- e. If appropriate, the recipient may be given information to empower them to safeguard the child in future.

94) If a person is not willing to sign the undertaking (Annex C), the police will need to consider if the disclosure should still take place. The outcome should be recorded and considered in the risk assessment and decision-making process.

95) At no time will written correspondence be sent out or left with the applicant or recipient in relation to the disclosure of information, as there would be a potential risk should such written information get into the wrong hands.

Disclosures when the applicant is not the recipient

96) In some situations, the applicant to the scheme may not be the person who is best placed to safeguard the child. In such situations, the applicant would not receive the disclosure or

be informed if a disclosure has been or will be made. The applicant should be informed that there is no information to disclose to them and be provided with guidance to stay vigilant and report any future concerns.

- 97) Consideration should be given to the privacy of applicants who are not the recipient of the disclosure. Where the recipient of the disclosure is not the person who applied to the scheme, the recipient should not routinely be informed who made the application or what information the applicant provided regarding the subject.

Self-disclosure

- 98) On occasion, the subject may wish to self-disclose. This may be by the subject making the disclosure to the applicant/recipient in the presence of the police. Alternatively, it may involve the subject making a disclosure to the applicant/recipient themselves and the police confirming that the relevant facts have been disclosed afterwards. Involving the subject in the disclosure may facilitate their understanding of the risk they pose of causing harm to a child and allow the subject to be part of their own offender management. Any decision in relation to self-disclosure will be recorded in the case management system and risk assessed accordingly.

Decision made not to disclose information

- 99) If a decision is made not to disclose information, then:
- a. The applicant should be told that there is no information to disclose to them given the information provided by the applicant and the result of checks made on that information.
 - b. However, it is important that the applicant is told that the lack of information to disclose does not mean there is no risk of harm to the child and the applicant should remain vigilant and report any future concerns. This contact also presents an opportunity to provide safeguarding information and signposting to relevant support services.
 - c. The subject will not be notified where there is no disclosure made.
 - d. The case should be finalised by the applicant being provided with a letter (Annex D) covering that there will be no disclosure and given a case reference number. Care should be taken about where the letter is sent to (particularly where the subject is living with the applicant). In some circumstances, it may be appropriate to deliver the letter in person to ensure that the letter does not get into the wrong hands. **Under no circumstances should personal data relating to the subject be included in the letter.**

3.9 Maintaining a record of the Disclosure Scheme

- 100) At the closure of every case (whatever the outcome or stage in the process), a final entry needs to be made to the case management system investigation log (which was created as detailed in [paragraph 35](#)) to record the request/information received, outcome, and details of all parties involved. This should serve as a piece of valuable information, which will be retrievable to all police forces via the Police National Database system to enable any patterns to be identified. From April 2021, it is mandatory for forces to provide data via ADR206 on the volume of applications and disclosures made.

- 101) If any named party involved in the CSODS investigation is a current ViSOR/MAPPS nominal, an entry must be added to their record. Details of any disclosure will also need to be added to the Disclosure Attachment on the ViSOR/ or the equivalent MAPPS Risk-Management Plan.
- 102) Any decisions made as a result of this scheme must be recorded fully and in a format that would stand up to the scrutiny of any formal review including judicial review.
- 103) It is also crucial that any relevant information coming to light as part of this process is shared as appropriate with all relevant agencies, in accordance with the principles of information sharing and disclosure as articulated in this guidance document.

3.10 Timelines

- 104) The maximum timescale for a CSODS investigation to be completed is 28 days from start to finish, unless extenuating circumstances exist which mean an extension is required and justified.

Right to ask		Right to know	
Initial contact made	Direct information received	Indirect information received	
Step 1 – Initial Contact checks	Completed within 24 hours from initial contact made		
Step 2 – Face-to-Face meeting	Completed within 10 days from initial contact		
Step 3 – Full Risk-assessment	Completed within 28 days from initial contact	Intelligence checks made	Completed within 28 days from indirect information received
Referral to local multi-agency forum occurs no later than 28 days from either step 3 – full risk-assessment (Right to Ask) or intelligence checks made (Right to Know)			

4. Definitions used within the scheme

- **Applicant** – the person making the application.
- **Application** – those enquiries that go on to be processed as formal child sex offender disclosure scheme applications. An application is made when the applicant provides the information required for the initial searches to take place, either in person, online, or over the phone.
- **Convicted of child sex offence** - for the purposes of this scheme means anyone convicted of, or cautioned, reprimanded or warned for an offence listed under Schedule 34A of the Criminal Justice Act 2003.
- **Disclosure** – includes both the disclosure of information about the subject’s convictions for a child sex offence and any other relevant information deemed necessary to protect a child or children from harm as listed in the scheme’s guidance document (e.g. serious domestic violence, child cruelty/neglect).
- **Initial contact** – the point when a member of the public makes an enquiry with the police with regards to making a disclosure application.
- **MAPPAs** - Multi-agency public protection arrangements are in place to ensure the successful management of sexual and violent offenders.
- **Registered sex offender** – a registered sex offender is a person convicted of or cautioned for a sexual offence against children or adults, who is subjected to notification requirements (commonly referred to as the “sex offender’s register”) that enable the police to monitor the individual.
- **Subject** – the person who the applicant is seeking information about who has some form of contact with a child or children.
- **Concerns** - this could include any of the following:
 - a. The subject has convictions for child sexual offences as listed under Schedule 34A of the Criminal Justice Act 2003;
 - b. The subject has other convictions relevant to safeguarding children (e.g. adult sexual offences, violence, drugs, domestic abuse);
 - c. There is intelligence known about the subject relevant to safeguarding children (e.g. cases not proceeded with or intelligence concerning sexual or violent offences, previous concerning behaviour towards children); and/or
 - d. There is concerning behaviour relevant to safeguarding children now being displayed by the subject or child that has been disclosed as part of the disclosure application (e.g. grooming or changes in behaviour that indicate sexual harm to children might be likely or sexual harm may have occurred).
- **No concerns** - where no convictions or intelligence relevant to safeguarding children and no concerning behaviour relevant to safeguarding children.