Procedure for viewing the social media accounts of children open to the Youth Justice Service

Effective Date: **06/02/2023**

Review Date: **06/02/2024**

Owner: YJ Service Manager

Links to other documents and policies

1. This policy does not supersede other Nottinghamshire County Council social media policies, and should be read in conjunction with the following NCC policies:

   Nottinghamshire County Council Social Media Policy
   Nottinghamshire County Council Social Media Guidelines

Reasons for looking at children's social media account

2. Occasional accessing **(i.e. no more than once in a three month period)** of the social media profiles of children with whom we work will provide intelligence regarding their activities, friendship networks and attitudes. This information can be used to assist with safeguarding the child and keeping those around them safe. Secondly, through accessing information that children have posted on a public forum, it will assist us to raise awareness with children of how to use social media safely and responsibly.

Criteria for looking at a child's social media account

3. The following criteria will be used to determine whether young people's social media accounts should be accessed.

   - Repeated missing episodes
   - Risk of Child Criminal Exploitation (CCE)
   - Risk of Child Sexual Exploitation (CSE)
   - Gang involvement
   - Credible risk of serious self-harm/suicide
   - Credible suspicion that conditions of bail/YCC/RO/YRO are being breached
   - Commission of a knife or weapons-based offence

4. There may be other circumstances where there is a credible risk to the child or others where it is judged that viewing the child's social media accounts would be critical to keep everyone safe. In these circumstances this will be discussed with the Team Manager

and management agreement obtained prior to any viewing. The reasons for the decision will be recorded on Capita by the Team Manager.

5. The viewing of child's social media accounts should be necessary and justified in all cases. Team managers should consider the whether the viewing of a child's social media profile is necessary and proportionate to keep everyone safe.

Process and frequency for accessing social media account of child

6. Children and their parents/carers are informed at the start of the intervention that their Case Manager may look at their public social media accounts on an occasional basis. The YJS Consent form specifically references that children's social media may be accessed and Case Manager's should make sure that children and their parents/carers understand this.

7. Children should be reminded of the accessing of social media posts as a minimum every three months (this could tie in with the Asset review where a child will be asked about any changes to their social media networks).

8. Children will have a right to object and, if this right is exercised, any further viewing of social media of that child should cease pending consultation with the NCC Information Governance Team. The Information Governance Team may consult the Caldicott Guardian in determining appropriate action. The child will be entitled to a formal response to their objection and the Information Governance Team will draft this in consultation with the Service and possibly the Caldicott Guardian and occasionally the Complaints and Information Team.

9. As part of the initial AssetPlus/OOCD/My Future assessment, children should be asked about which social media platforms they use, and this recorded in the 'networks' section of the AssetPlus. For OOCD and My Future assessments, information about social media use should be recorded as part of the 'lifestyle' section.

10. If a criterion arises whereby a Case Manager considers that viewing the social media of a child is essential to keep everybody safe and meets the criteria outlined above, the Case Manager will discuss this with the Team Manager, who will make an entry onto Capita with the reasons for the decision.

11. **Social media accounts may only be viewed a maximum of once in every three-month period and Team Manager authorisation must be gained on each occasion.**

12. Viewing of a social media account on a more frequent basis constitutes surveillance. The Regulation of Investigatory Powers Act (RIPA) must be followed if it is considered that surveillance is required. RIPA allows for 'directed surveillance' when it is necessary and proportionate, for the purposes of detecting or preventing a criminal offence punishable by over six months in prison. The authorisation must come from an authorised officer of the Council after taking legal advice. **The Nottinghamshire County Council RIPA policy must be followed in these instances.**

13. The Case Manager will use their own personal social media account to look at the public profile of the chid. If the Case Manager does not wish to do this or does not have a social media account on the platforms used by the child, a request can be made of the Team Manager with social media responsibility to meet (face to face or virtually) to complete the checks on their behalf.

14. The Case Manager will then follow the process outlined in Appendix 1.

Incidental Intrusion of other people's data

15. The focus of the social media monitoring set out in this procedure is young people who are service users of the Youth Justice Service. Given the nature of social media however, it may well be that looking at a young person's account will also mean that other people's data is accessed (e.g. family networks, friends etc).

16. These peripheral networks of friends and family are not the intended focus of the social media monitoring. Information gained about, or in respect of, individuals in peripheral networks will not be processed in any way beyond incidental viewing (i.e. will not be collected, shared, reported on, stored etc) unless there is a significant safeguarding concern which necessitates such information being processed.

17. Where this incidental information is processed, it will need to be at the authorisation of a Team Manager and the rationale the fully documented on Capita, in line with the provisions for recording monitoring undertaken elsewhere in this document.

Social media platforms and keeping personal data/identity safe

18. Case Managers will not be compelled to use their own social media accounts to access those of service users. To do so is entirely voluntary and a matter of choice.

19. Service / Team Managers will provide Case Managers with information to enable informed decision, based on known risks, about whether to use their own personal accounts for accessing social media accounts of young people.

20. Case Managers should not 'friend', 'follow' or 'subscribe' to the social media accounts of the children with whom they are working or their family members.

21. In order to keep their own data and identity safe, Case Managers should review the privacy settings of their social media accounts.

22. Case Managers should familiarise themselves with the privacy settings of any social media platform prior to viewing a child's account to ensure that personal information will not be exchanged (for example the child being able to identify the personal social media account of the Case Manager following the viewing).

23. The following list includes the most popular social media sites used by children and the current privacy options provided. [Last checked 03/01/2023]

Platform	Privacy Settings (at 03/01/2023)
Facebook	• It is not possible to identify who has looked at your Facebook account or for anyone else to see that you have looked at their profile. • A Facebook account must be linked to a real person and their terms and conditions specify that a user should not provide a fake profile. • To view the profile of someone else on Facebook, even if public, Facebook is set up to encourage a viewer to have an account.
Instagram	• It is possible to see who has viewed 'stories' on Instagram. It is not possible to see who has viewed the regular page. • There are some 'apps' who offer users the ability to see who has viewed their profile. These are paid for apps and it is not clear whether they can actually provide this information. Instagram deter people from using these apps. • Instagram do not have any rules regarding linking to account to an identifiable person and it is thus easier to be anonymous using this platform. Users often do not use their own name, so knowing the account name is useful.
YouTube	• It is not possible to see who has viewed film uploads on YouTube. • You do not need to have a YouTube account to view films that users have uploaded or to search for 'channels'.
TikTok	• Users can see who has viewed a profile if the viewer is logged into an account. • Searches can be made from a web browser if the account name is known. However, this is unlikely to be a user's own name so knowing the account name is useful.
Twitter	• It is not possible to see who has viewed a Twitter profile. • Anyone can partially view a Twitter profile without having an account, but an account is needed for viewing the whole profile.

Reviewing of the business practice of monitoring social media accounts

24. The monitoring of young people's social media accounts will be **reviewed on an annual basis** by the Service Manager (or their nominee). This review will as a minimum test the following assertions:

- There continues to be clear, documented benefits to undertaking the social media monitoring of young people's social media accounts;
- Appropriate action has been taken in light of any complaints / concerns / objections raised about the monitoring of social media accounts both in terms of the individual concerned and in terms of the wider service approach;
- Local procedures are working well and are not in need of refinement

- Clear records are being maintained as an audit trail of monitoring young people's social media accounts.
- Risks associated with the approach have been assessed and have been effectively mitigated to an acceptable level or are being tolerated.

25. The review will be documented and will be forwarded by the Service Manager (or their nominee) to the Information Governance Team who will store it with the relevant Data Protection Impact Assessment (DPIA) documentation.

26. The Service Manager or Team Managers will ensure that the monitoring of young people social media accounts DPIA is amended and used to document privacy considerations of any material amendments to the data processing as currently described in the DPIA.

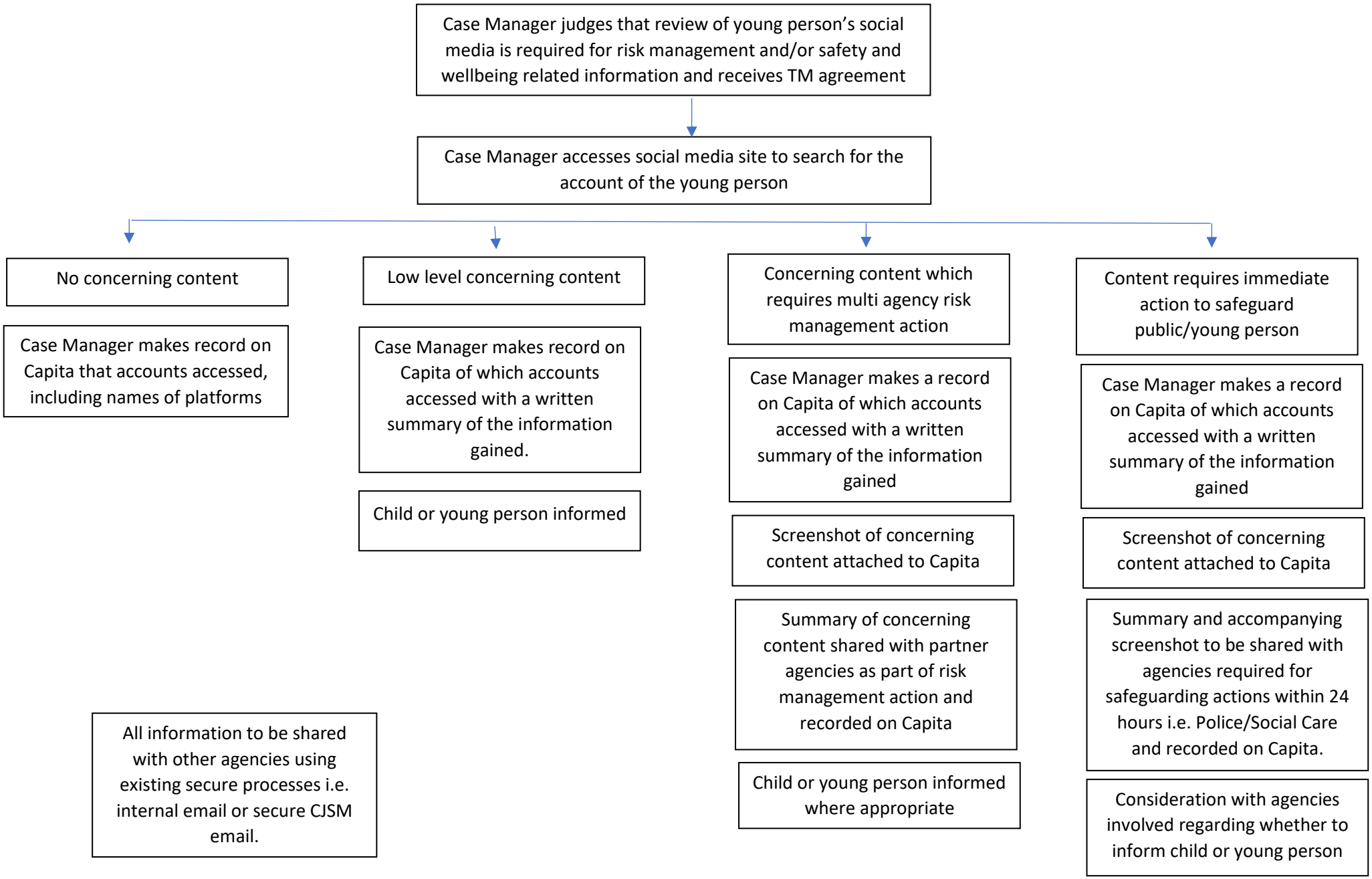
27. Data protection impacts need to have been properly considered and documented in the DPIA prior to any material changes in the way personal data is being processed.

Document Control

Owner	Youth Justice Service Manager
Author	Sarah Parr
Last Reviewer	Sarah Parr
Approver	Youth Justice Service Manager
Date of Approval	
Date of next review	06/02/2024
Version	2
Classification	Public (when approved)

Version	Date	Changes
2	06/02/2023	Updates to social media platform privacy policies. Change of wording from 'risk' to 'keeping everybody safe' to align with YJ policy principles.

Appendix 1


Case Manager judges that review of young person's social media is required for risk management and/or safety and wellbeing related information and receives TM agreement
Case Manager accesses social media site to search for the account of the young person
No concerning content
Case Manager makes record on Capita that accounts accessed, including names of platforms
Low level concerning content
Case Manager makes record on Capita of which accounts accessed with a written summary of the information gained.
Child or young person informed
Concerning content which requires multi agency risk management action
Case Manager makes a record on Capita of which accounts accessed with a written summary of the information gained
Screenshot of concerning content attached to Capita
Summary of concerning content shared with partner agencies as part of risk management action and recorded on Capita
Child or young person informed where appropriate
Content requires immediate action to safeguard public/young person
Case Manager makes a record on Capita of which accounts accessed with a written summary of the information gained
Screenshot of concerning content attached to Capita
Summary and accompanying screenshot to be shared with agencies required for safeguarding actions within 24 hours i.e. Police/Social Care and recorded on Capita.
Consideration with agencies involved regarding whether to inform child or young person
All information to be shared with other agencies using existing secure processes i.e. internal email or secure CJSM email.