SCOTTISH CHILDREN'S REPORTER ADMINISTRATION

Scottish Children's Reporter Administration Minute of Information Governance Leads held on Tuesday 21st February 2023 via Microsoft Teams

Present:
Alistair Hogg (chair), Angela Mitchell, Hannah McCulloch, Janet Robertson, Jacqueline Johnston, Stephen Eodanable, Bruce Knight, Nicola Baird, Gwen McNiven, Victoria Ritchie, Jo Donald, Kelly Campbell, Ed Morrison, Fiona Combe, Ellen Young, Paul Mulvanny (left after item 10) and Gill Short (joined at Item 5 and left after item 10)

		Timescale	Action
1.	**Apologies** Donald Lamb, Jacqui Stephen, Pamela Armstrong, and Helen Etchells. AH welcomed Fiona Combe and Ellen Young.		
2.	**Any other Business** Two items added and dealt with at the end of the meeting: **i) Bruce Knight - Current Security Issues** **Removal of GSI –** BK stated that there are still organisations sending child information using SCRA's old GSI email address. Locality lists have been provided to identify these senders to encourage them to only send to email accounts that belong to the scra.gov.uk email domain. Courts are still sending to both addresses. Scottish Councils are no longer using the GSI and have secured their current email domains appropriately so they can continue sending child data to SCRA securely. The removal of gsi will occur at the end of the March 2023. **Security Awareness Training/Champions –** Security Awareness Champion training places are available and would be encouraged for Locality IG Leads. Anyone interested should contact AH. **Simulated Phishing Exercise** - BK referred to the recently circulated phishing campaign report. SCRA performed well compared to many other organisations. There are Bite-Size videos on Connect that will assist staff on recognising phishing attacks from the normal business emails they usually receive. **Security Critical Update** – This is available for users to self-install at a time convenient to them and thereby avoiding the scheduled install interfering with their work. **BDO Audit actions. -** There are 4 findings and with some progress being made on each action. One of these actions requires the IG Leads group to become the Cyber Security Steering Committee, allowing them to be aware of any Digital Security and Governance tasks so they can comment on their operational impact. **ii) Hannah McCulloch –** Summarised the recent Locality Focus Group held in South East. This summary is to be circulated with the minutes. AH commented that even if things are relatively stable, these focus groups can be really useful.	**ASAP**	**All**
3.	**Minutes of last Meeting (22nd November 2022)** Accepted as correct **Matters arising** <u>Updates on actions from previous minutes</u> **CSAS warning box-outcome of locality input** – SE updated. SOM was updated in December 2022 with an instruction to check for any ND/PI warnings in warning box and to review and delete any warning note no longer applicable and add date to any new warning added. Was this enough or does it need to go further? A discussion followed. JJ noted that Reporters are concerned that certain things such as somebody about to leave prison, should not be hidden away and the warning box makes such information very visible. SE invited Paul or Alistair to		

		Timescale	Action
	comment on whether there could be Locality level uses that were not within the SOM. PM said that the SOM can be amended but irrelevance needs to be avoided and accurate records must be maintained. 'Customer Care' issues need to be put somewhere and he is open to looking at it and not necessarily adding things onto the SOM. VR & FC added that an 'additional information' tab would be useful but needs to utilise specific terminology with good housekeeping to prevent any out-of-date issues. It is important to know things like bail conditions at a glance. Key words would be helpful. AH suggested there was more scope to allow more of a use but not to overload the warning box. We need to look at risk again. It should only be non ND risks e.g. Health and safety reasons at a hearing. We need to be mindful that we don't dilute the use or benefit of the warning box as it is now. ND is always the most important risk. Agreed that comments should be with Stephen by the end of the week.	**ASAP**	**All**
4.	**Deletion of duplicate contact records - test of change** SE – Duplicate contact records are being discussed within the Data Quality Group. The SOM requires a check of existing contact records before creating new records. The Digital Team are looking to improve the functionality of the search. We then need to deal with old records. It used to be the CSAS Helpdesk that dealt with these. There is a new process which is going through a test of change with Jim in Hamilton likely to assist. Duplicates will be marked 'do not use' (SOM will reflect this). LSMs in Hamilton will unlink duplicate links. They will indicate who has dealt with the record by adding their initials. The Digital Team will run a monthly check. This should reduce creation and make it simpler to delete existing duplicates. Once the test of change is complete SE will report back to the Digital Quality Group. SE should hopefully know more by the next IG Leads meeting but August at the latest.		
5.	**Retention of case information after 18th birthday (impact on multi-agency reviews)** AH - CSAS auto deletion has commenced and this is a fantastic advance for SCRA. SE is looking for any comments from Localities. 78 cases were already marked for retention prior to the 22nd February deadline. Five or six were accepted for review and these will require further details to be provided to see if they meet the new higher threshold for retention. It cannot be assumed that just because it was marked for retention that it will be retained. The cut-off date is 15 days after a person's 18th birthday. It is hoped that other partner agencies will understand how careful we are. SB asked if a report will be generated and sent to Localities to ensure over 18's paperwork is cleared out? SE will clarify with DL, but yes, reports are available.	**ASAP**	**SE**
6.	**ND Group Workstreams** AH - The focus group hasn't met since November because they had concluded significant work around recording Statutory documents and CSAS producing documents in a pre-redacted form. They will meet next month and see how the work completed is reflected in breaches. AH asked if there had been any issues with the rollout of the completed work and had anyone noticed any discernible difference, particularly regarding the Hearing Outcome Notifications? KC commented that after an initial apprehension of the new process it has been fine. She thought that the annexe would cause more work but to date she is unaware of any additional work. JR concurred that Ayrshire have not been asked for any annexed documents. VR asked if there are two versions required for Social Work. Grampian are sending one version to SW as they are already in possession of the information. There will be a 6 month period of monitoring this procedural change.		

		Timescale	Action
7.	**6 Monthly Report summary** JD delivered a summary of the 6M report that had been circulated prior to the meeting.		
8.	**IG Leads Development Day** Agreed to revisit this in 6 months.		
9.	**Annual cyber-security refresher training** BK explained that the SG Introduction to phishing scams | SG Thrive (learn.link) eLearning course is to be completed and this must not be confused with the Nexus Cyber-security course available through SCRA's training platform. A list will be sent to IG Leads monthly of non-attendees or those who didn't complete the training. Staff are to be made aware that if the survey at the end of the training isn't completed, they will be registered as not completing the course.	**Monthly updates**	**BK**
10.	**USB Sticks** BK is looking for volunteers for the QA group to assist them with evaluation of the new USB controls put in place to implement the new SG security policy. BK explained that there are 2 different types of access available for USB sticks. Read access is the default access for all SCOTS users and write access requires a business case supported by the relevant Information Asset Owner. An approved support officer could write info from the SCOTS environment to the USB stick to be read later. There are currently over 200 USB SCRA approved sticks in circulation across SCRA and although these will be supported initially by SG they could not guarantee that they would always work with the new SG security policy. Replacement to the SCOTS approved type of USB stick at £70 each would be a significant cost to SCRA. There would need to be a minimal list of those with 'write' access or it defeats the security policy aims. A lengthy discussion followed about the merits of USB stick usage. PM explained that sticks are distributed to agents as video interviews are shared via USB sticks. This information originates from the Police, so a conduit arrangement is required. PM asked if A to B via file transfer is technically 'writing'. BK is not sure if a transfer from USB stick A to USB stick B to avoid the need for writing permissions is possible. SCOTS laptops have 2 USB ports and at least one of these is usually in use. If a docking station is used then this may offer additional USB ports. These are the type of scenarios that need to be tested as part of the evaluation by the QA group so we can understand the limitations of this new policy. BK stated that a transfer from a Police USB stick to a secure JII folder on SCOTS is considered a read process. There is a JII procedure on this process so that video evidence can be transferred to SCOTS for storage. The Police provide a USB stick with an integrated keypad (this is the SCOTS approved USB stick) and they enter the PIN on the Keypad to allow the transfer to SCOTS to take place and then leave with their USB stick. The supply of this Police evidence to Defence Agents would require someone with write permissions to transfer the data from SCOTS to the USB stick. PM acknowledged the need for other solutions to be explored as this is a risk. AH wanted to explore the least impactful way of getting to the necessary outcome. The QA group need to look at potential solutions, with volunteers from Localities who understand the localities dependence on USB sticks. There is a need for several locality staff to join the QA group to evaluate the proposed changes and determine who in the locality will need write access to USB sticks. JR offered to join the group as this is part of their work but not significant. If there are others who use USB's they might be better placed to join. KC is the person in her office who copies information onto the G:Drive, copies the sticks and tracks them. VR said Grampian has spates of them, e.g. six in two months and then none for ages. It is simple to do but she was trying to work out how best to contribute. SB commented that there is not a high number with H&I either. PM noted that to		

		Timescale	Action
	expedite matters, staff have shared memory sticks with agents. This could be higher than imagined and it should be made easier to invite people into offices to view video material post-Covid. KC agreed that one of the difficulties is getting a shared stick back from solicitors. BK then spoke about Objective Connect for sharing but the Courts won't accept this yet, despite Donna's work in this area. For defence agents we should use Objective Connect. There was an agreement that solicitors are used to viewing this material away from the office. JS commented that solicitors shouldn't get another stick until they have returned the last one if there is no reason to retain it. She is aware of an undertaking referring to this. JJ asked if it had to be an IG Lead or if someone more appropriate from Locality could join the QA group? This would be possible, and PM agreed it would be helpful to involve the JII Leads.		
11.	**Examples of good Locality practice or issues arising** BK asked about the popularity of the Bite-Size videos on Connect. They are generally well received.		
12.	**New risks** Change around USB sticks was identified as a new risk. VR noted the limited access to shared contacts as a risk. The significant amount of time spent tracking down the 'owner' of records and updating warning boxes. This is further complicated where a warning was put on a child's record but the child has siblings in different Localities with different contacts. The person with Global Access wasn't available to make the updates. There are role-based access issues in Grampian but this is probably a wider issue. AH noted that there are good reasons why role-based access is in place, but this could cause a bigger risk in some circumstances. We need to revisit this issue and have a more detailed exploration.	**By next meeting**	**All**
13.	**Date of Next Meeting - Tuesday 23rd May 2023 via Teams @ 13:30** AH thanked everyone for attending the meeting.		