Scottish Children's Reporters Administration
Agenda of Executive Management Team Meeting
Held on Wednesday 08 January 2020, 10:30-1:00pm
at Bell Street, Glasgow

AGENDA

		Paper	Action
1.	**Apologies**		
2.	**AOB**		
3.	**Minute of Previous Meeting 04 December, 2019**		
4.	**Matters Arising**		
5.	**Budget 2020/21 Draft Board report – For review**		EM
6.	**Feasibility Studies – For discussion**		EM
7.	**Self-assessment on** • **performance /objectives for 2019/2020** • **Objectives 2020-23** **– For discussion**	Verbal	NH
8.	**Draft Board Agenda – For Review**		NH
9.	**Draft Remuneration & Succession Planning Committee Agenda – For Review**		SD
	Standing Items		
10. a) b) c) d) e)	**Digital Programme** Organisational Readiness update Data Migration programme DDOC/DDB Capacity planning Communication and Operational update		 TP/PM NH NH TP/SD TP
11.	**Information Governance** a) Annual training of data protection in respect of staff records – For approval b) SCRA Role-Based Access Rules for CSAS – For review c) CSAS Password Policy – For Review		 AH AH AH
12. a)	**Practice and Policy** Advocacy Communication – For information and discussion		 AH

13.	**New Risks**	Discussion	All
14. a) b) c) d) e)	**Forward Look** Care Review Event 09/01 CHS/SCRA Senior Teams Workshop 10/01 Justice Board 16/01 Rem Com & Board 29/01 ACR Programme Board Meeting		
15.	**Items for February meeting and afternoon session if required – For discussion**		
	Date of Next meeting; Wednesday 05 February at Ochil House		

Scottish Children's Reporter Administration
Executive Management Team
04 December 2019

Present:

Neil Hunter (NH) - Chair
Susan Deery (SD)
Tom Philliben (TP)
Helen Etchells (HE)
Ed Morrison (EM)
Lisa Bennett (LB)
Paul Mulvanny (PM) – by VC
Pamela Armstrong (PA) by VC - Minute

		Timescale	Action
1.	**Apologies** None		
2.	**AOB** **Case Sampling** Approval given from ARC to skip two quarters of case sampling due to CSAS Deployment. NH to go back to ARC to ask for approval for an extend embargo to 3 quarters.	**Feb 20**	**NH**
3.	**MOLM** Agreed as accurate.		
4. a)	**Matters Arising** New email domain name AH sent info to EMT advising the switch over will be 13 December. Lots of reassurance given around testing done in advance and looks to be comprehensive. Safeguards in place, e.g. redirection of emails for a shot term of time.		
5.	**Procurement Report** EM introduced the report, asking EMT to note Procurement activity during the first six months of 2019/20 and further planned activity which further aligns SCRA with Scottish Public Sector best practice.		

	Issues arising from discussion: • Need for ongoing good relationships and proactive communication between procurement team and contract leads **Agreed:** • 6 monthly progress report noting risk, role and expertise will be brought to EMT	**Jun 20**	**EM**
6.	**Temporary Contracts** AH introduced the item. **Issues arising from discussion:** • Concerning the extension of contracts, the right arrangements are in place however, there is a timing issue with a number of contracts ending in March 2020. • We have been advised of a budget delay until the end February potentially end of March. There is an anxiety we have not been asked to provide forecasts to SG. • There are temporary contracts across head office and localities with some contracts already extended until September. • Temporary staff may move on to roles external to staff • The need for decisions to extend contracts beyond current timelines in the IT team as core and extended testing requires more certainty in available resources.		
7.	**OHOV** AH introduced the item. **Issues arising from discussion:** • This is an appropriate time to review the stage of development of OHOV • Review of structure of OHOV team including project leads role and the level of professional support is required. • ongoing work to strengthen safeguarding policies. • ongoing review of skills mix and group members support needs in a reconfigured staffing arrangement broadly within the existing budget		

	• We need to understand what is being taking on and ensure the correct supports are in place for staff, managers, and Young People. **Agreed:** • Consider type of contracts required and Report back to EMT • Committed to making Project Lead permanent. This will be taken to the Establishment Group. • Bring any configurations into existing budget. SCRA should receive some of the income from SG.	**Feb 20**	**SD/AH/LB**
8.	**Corporate Planning – EMT Planning Session** Workshop arranged for the afternoon of 08th January. The first draft of the plan will be taken to the January Board.		
9.	**Review of December Board Reports** Draft Board Reports were reviewed.		
	Standing Items		
10. a) b)	**Digital Programme** Organisational Readiness update • Highlight report to be sent to EMT. There is a strong sense of progress, assurance and optimism about development. Good, steady progress is being made with nothing of major concern. • The issues around redaction and SharePoint are coming along. • What is the clear roll back position? Do we roll back or work around? There is work to be done in relation to this. • The product is being tested next week and will be handed over to the core team 09 December. The team will then be able to assess further technical details. • Training plans are looking well formed. Capacity planning • Managers will need to be flexible and adaptable around holidays and childcare.		

11.	**Information Governance** AH provided the following update • Regarding a referral made to ICO, no action to be taken and recommendations given which are already in place.		
12. a)	**Practice and Policy** Research Proposal and Data Analysis: Under 12s in Residential Care AH introduced the report that will be taken to the December Board.		
13.	**New Risks** The following potential risk were identified and will be assessed. 1. Future changes to the Hearings system. 2. Operational child protection risk around OHOV		**NH/AH** **LB/SD**
14.	**Forward Look** The forward plan was reviewed.		
	Date of Next meeting 08 January 2020, Bell Street		

SCOTTISH
CHILDREN'S REPORTER
ADMINISTRATION

Accountable Director: Head of Practice & Policy **Date:** 17 December 2019

Report Author: **Colette Cairns**
Personal Information Officer

Recommendation:

1. **For EMT to approve the annual training of data protection in respect of staff records.**

Reason for Report: *Requested by EMT*

Resource Implications: *Within approved budgets*

Strategy: *Within approved plans*

Consultation: *EMT*

Equalities Duties: *No Equalities impact assessment required*

Document Classification: *Not protectively marked*

1. Introduction

1.1 GDPR (General Data Protection Regulation) and the Data Protection Act 2018 came into force in May 2018, the new legislation requires organisations to evidence that they are complying with the Data Protection Act. In addition there is a requirement to provide annual GDPR training to all staff, the ICO (Information Commissioners Office) has also recommended that more role specific training should be provided to staff.

1.2 SCRA has developed and delivered a number of role specific training for staff, as part of this, sessions were delivered on how we deal with data protection of staff records.

2. Background

2.1 In order to develop this training, SCRA's data protection policies were considered along with legal requirements involving staff records. The training was developed with consultation between HR, Unison and the I&R team.

2.2 The training was delivered between April and July 2019 to the EMT, LRM's, LSM's, HR personnel and staff who deal with staff records. Following this training, the EMT requested that there should be a review carried out to assess the effectiveness of the training.

2.3 After some thought on how we could monitor and ensure that procedures were being following, it was decided that a survey be sent out to all the staff who participated in the training.

The survey was launched in July and requested a response by the end of August

3. Survey results

3.1 Of the 80 members of management/staff who attended the data protection training, 37 completed the survey, equating to a response of 46%. (appendix 1)

3.2 The responses were positive and indicated that much of the course was retained, and SCRA policies are in principal being adhered too.

100% of respondents were aware that staff records included: Occupational health reports, Appraisal paperwork, Supervision notes and Capability investigations. 89% knew that Flexi sheets should be retained for 2 years from the date signed off, 72% that Performance management records should be kept for 4 years and 81% that personal HR files are kept for 6 years from the date employment ceased.

It was of interest to see that 59% had cleared/deleted their sent items email box within the last 3 months and that 56% only had emails of less than 12 months old in their in box. Prior to the training this was something many admitted to neglecting.

The majority of responses, 86% were aware of where to find guidance on the retention of staff records.

3.3 An area which needs to be re-addressed would be the reporting of staff breaches. At the training is was emphasised that staff breaches should not be sent to the breaches mailbox and should be dealt with by the Data Protection Officer in the first instance. However, 35% of respondents said they would contact the breach mail box, which is not the policy.

4. Concerns raised

4.1 Unison have raised concerns regarding details of staff information being widely known between managers, some from different localities. This raises the issue that whilst managers are aware of SCRA's policies, they are not being adhered too in practice. 75% were aware that an email containing information about a private matter which may impact on their work, should be saved into their H drive and deleted from the inbox, ensuring the information is not available to others. However, this does not seem to be applied when discussing staff information. This highlights the need to re-inforce not only the data protection training but also the fact that SCRA has recently updated its Dignity at Work policy.

5. Unison

5.1 Unison provided the following paragraph regarding staff confidentiality.

Protection of Staff personal data is paramount if the organisation is to maintain credibility within the staff body and adhere to its GDPR responsibilities, therefore the importance of restricting the sharing of personal information cannot be emphasised strongly enough.

UNISON recognises that, for managers within a locality, it may be necessary to disclose personnel issues to ensure operational requirements are met. However, it is important that these discussions are restricted to only that which is essential to the operation of the locality and to any person who has an absolute need to have that information. It is recognised that where there is a requirement to refer matters concerning staff to other departments within the organisation the expectation is that confidentiality should be maintained at all times.

UNISON is committed to working with SCRA to ensure that initial training and refresher training continue to be delivered to staff who hold any personal data on other staff members.

6. Recommendation

6.1 To ensure that managers are not only aware of the data protection of staff records policy within SCRA, but that these are also being implemented, I would recommend that data protection training on staff records should become part of the annual training for managers and those who deal with staff records.

I would propose that this is done via an E-Learning Course, and an annual refresher session which could be delivered at one of the LSM and LRM network meetings.

The ICO have recommended that we consider:

- ***Reviewing the content and frequency of your data protection training to ensure that all staff receive regular practical guidance in the application of their data protection obligations.***

Whilst this recommendation was not in relation to staff records, the same principal applies with regard to our obligations.

APPENDIX 1

SUMMARY OF SURVEY

1) Which of the following are staff records?

	Responses
	94.59%
Occupational health reports	100.00%
Appraisal paperwork	100.00%
Bank details	91.89%
SCRA email address	45.95%
Supervision notes	100.00%
iTrent information	91.89%
Next of kin details	91.89%
Capability investigations	100.00%
Complaint about staff	91.89%

2) How long would you retain the following records for?

	2	4	6	8
Flexi sheets (from date signed off)	89.19%	10.81%		
Performance management records	5.41%	72.97%	21.62%	
Grievance procedures (from date of last action)	8.11%	8.11%	75.68%	2.70%
Personal HR files (from date employment ceased)	5.41%	10.81%	81.08%	2.70%

3) What information about a staff member is their personal data?

	Responses
Staff employee number	54.05%
Name, address and NI number	97.30%
Locality office	16.22%
Appraisal records	91.89%
References	86.49%
Religion	83.78%
SCRA email address	24.32%
Trade Union membership	89.19%
Sexual orientation	89.19%
Attendance at training records	54.05%

4) How long does SCRA hold staff personal records for after Termination of employment?

Answer choices	Responses
2 years	8.11%
4 years	5.41%
6 years	83.78%
8 years	2.70%

5) What is the oldest email in your inbox?

	Responses
Less than 3 months	24.32%
Between 3-6 months	8.11%
Between 6-12 months	24.32%
Older than 12 months old	43.24%

6) When did you last delete/clear your sent items email folder?

	Responses
Within the last 3 months	59.46%
Within the last 3-6 months	10.81%
Within the last 6-12 months	8.11%
Longer than 12 months ago	10.81%

7) What should you do upon receipt of a staff members sickness certification?

	responses
Keep it	
Scan a copy and sent to payroll Mailbox, returning original to employee	97.30%
Review and return to employee	
Scan a copy, send to payroll mailbox and destroy original	2.70%
Destroy it	

8) Where should you find guidance on the retention of staff records?

	responses
Practice guidance	
Information Security handbook	13.51%
Records Management policy	86.49%
Employee and Managers handbook	24.32%
Record of Processing Activities	21.62%
Data Protection Act 2018	27.03%
There isn't any	

9) Who would you contact in the event of a breach of a staff members' personal data?

	responses
Breach mailbox	35.14%
Principal Reporter	2.70%
Data Protection Officer	89.19%
HR	78.38%
Senior Information Risk Owner	29.73%
SOM or Head Office senior Manager	35.14%
The staff member concerned	81.08%
Locality Management Team	24.32%
UNISON	2.70%

10) Where should you store Performance Management Records?

	responses
G Drive	5.41%
H Drive	7027%
Locked filing cabinet	64.86%
Main filing room	
On the desk	
iTrent	51.35%

11) A staff member has emailed you to let you know about a private matter that may impact on their work. What do you do with this email?

	Responses
Save it to your H Drive and delete from your inbox	75.68%
Forward it to the rest of your Locality Management Team or other Head Office Managers	
Forward it to the rest of your team	
Keep it in your inbox	8.11%
Forward it to HR	32.43%
Forward it to Senior Operational Manager or senior Head Office Manager	
Keep in your sent items (if forwarded)	
Delete without reading it	2.70%

SCRA Role-Based Access Rules for CSAS

This proposal is derived from the embedded presentation and workshop held on 22/10/2019. Given the potential for complexity, which in itself is a risk i.e. if the solution/implementation is hard to understand and/or maintain, then the first rule we are seeking to establish is:

Rule 1. 'Simplicity in relation to Role-Based Access Control'

Job Roles: Locality Teams comprise relatively few job roles but the functions carried out, though broadly divisible into support and reporter activity, have some degree of variation in terms of who does what and/or in what order e.g. first check/second check of redaction. There are also many more 'national' roles with disparate functions.

Personas: There is the potential for a 'persona' to be created for the acting out of any feature or job function, whether it is operational in nature e.g. child record creation, or based on a security and information governance requirement e.g. review audit information.

Between **Job Roles** and **Personas** there could be devised a complex model of security groups and related permissions, resulting in a matrix of permutations that accounted for the locations in which each given individual works, as well as how they carry out their purpose and functions within CSAS.

Security Model: The products that comprise CSAS provide for such granularity, offering a security model combining concepts of organisational structure (**role based**), layered with **record based** constraints, right down to the level of **field based** restriction.

Operationally though, the currency of access is relatively binary, either a member of staff needs access to the electronic equivalent of a 'child's file' or they don't, calling for a very simple but rigorous set of rules.

Rule 2. 'A child's file is the unit of processing, with the associated child contact record the gateway to access'

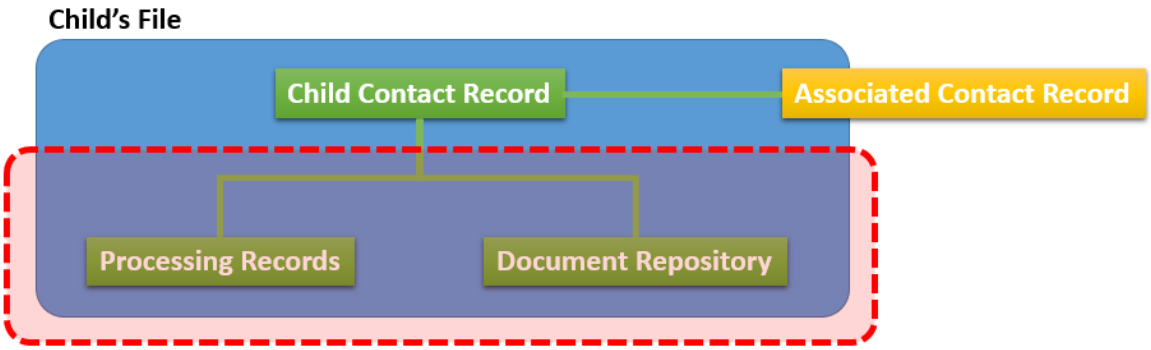

Figure 1. Child Contact Record in context of Child's File

Though there are subtleties in practice, generally all of the components that comprise a 'child's file' must be accessible and/or be able to be acted upon when processing that 'child's file', regardless of job role. With regard to the principle of **least privilege**, what a user 'needs to know' is effectively 'everything in respect of a given child' if they have (or are likely to have) processing duties in respect of that child.

Child's File: a 'child's file' is all that cascades from the core 'child contact record' (structured data[1]). Associated with this core identifying record, are a dozen or so other types of (structured) record that comprise the processing activities in respect of that child i.e. representing decision making, case progression, meetings and outcomes. The child's document repository (unstructured[2]) i.e. reports and other information submitted from third-parties in respect of that child also fall within the boundary and description of that 'child's file'.

Child Contact Record: Importantly, as a national service all SCRA staff may need access to a 'child's file' but will 'need to know' of the existence of all children[3]. All SCRA staff with processing duties will therefore be able to access the core identifying 'child contact record', which may lead to access to all of the related records and documents that constitute the 'child's file'. For the same purposes, any 'contact record' of a person (containing nominal information to identify that person and their relationship) that is an 'associate' of a child will be transparent to all SCRA staff.

Rule 3. 'The active reporter is considered the owner of all that comprises a child's file, whilst there is ongoing processing activity'

The concept of ownership of a 'child's file' cascades from ownership of the 'child contact record'. All[4] processing records and documents associated with the child contact record, have the same allocation of ownership. The 'active reporter' nominally identifies the decision maker in respect of a given child, and by default is the system user alerted to the events, tasks and generally has visibility of the processing activity within the 'child's file'. Ownership, does not preclude other users processing that 'child's file' or seeing the activity.

Rule 4. 'Access to a child's file is determined by it being active, and constrained only to the active reporter and their peers within a Locality'

Active/Dormant: A 'child's file' is 'active' when there is processing activity e.g. in-flight referrals, hearings, proof, appeals etc. and/or when the child is subject to compulsory measures. A 'child's file' is considered 'dormant' when the converse is true and by definition cannot have an 'active' reporter, and consequently cannot be

[1] Structured data resides in a fixed field within a record, organised into a formatted repository, typically a database, so that its elements can be made addressable for more effective processing and analysis
[2] Unstructured information either does not have a pre-defined data model or is not organised in a pre-defined manner. Unstructured information is typically narrative-heavy.
[3] With rare (1 in 5,600) 'restricted' exceptions
[4] Associated Contact Records can have an affiliation to more than one Child Contact Record, and are not 'owned' by a named individual

accessed. Notwithstanding that all users can read and/or act on all 'child/associated contact records', 94% of children's files will not be routinely accessible.

Operationally, all members of a Locality Team, irrespective of role are likely to have duties in respect of a 'child's file' while that record is active, and the owner/active reporter is a member of that Locality Team. Complexities aside where staff bridge multiple Localities, a 'child's file' is therefore accessible/actionable at the level of the Locality.

The table below approximates per Locality, the scale of access that follows from this rule in term of how many users each have access to how many active children's files at a given point in time:

Locality	Number with access	Number of children's files
Ayrshire	59	1402
Forth Valley	46	1260
Glasgow	87	2238
Grampian	34	774
Highlands & Islands	31	825
Lanarkshire/Dumfries & Galloway	56	1834
North Strathclyde	60	1927
South East	43	1754
Tayside and Fife	55	1623

Table 1. Scope of Access

Rule 5. 'The archiving of a child's file into a dormant condition and it's retrieval to an active condition is both well governed and operationally efficient'

Archival/Retrieval: Rule 4 systematically constrains access to the greatest majority of sensitive information held within CSAS. Accounts with permission in relation to dormant records will effectively be responsible for (and vulnerable to) providing access to an archive of 94% (approx. 180,000) of children's files. Compared to the scope of access set out in Table 1, any account with this level of access must be considered to have elevated-privilege and as such the governance practices associated with retrieval in particular, should be restrictive, close to but short of the point of being operationally oppressive.

Rule 6. 'Gaining exceptional access to a child's file is both well governed and operationally efficient'

The proceeding rules set out the parameters for a routinely simple model of access to children's files. Exigencies of operational practice, and in particular with regard to non-routine access i.e. for national roles, it will be necessary to extend access to a child's file to additional users. Given the necessary and sufficient scope of access shown in Table 1, it would be reasonable for the Locality Team (or a limited subset of its membership) to routinely manage the sharing and removal of non-routine access.

Rule 7a. 'Special considerations apply to any child contact record which specifies Non-Disclosure provisions'

Non-Disclosure: As expressed previously in Rule 2 all SCRA staff 'need to know' the nominal identifying information provided in every 'child contact record', and this extends to knowing if a non-disclosure provision is in place. By definition, non-disclosure provisions only apply to 'active' cases but since all staff have access across Localities to the 'child contact record' which details the specifics of the provision beyond simply identifying that there is a provision, then protection of the specifics to within a Locality is of special consideration.

Locality	Number of ND provisions
Ayrshire	95
Forth Valley	73
Glasgow	206
Grampian	59
Highlands & Islands	55
Lanarkshire/Dumfries & Galloway	190
North Strathclyde	147
South East	142
Tayside and Fife	159
TOTAL	**1067**

Table 2. Scope of ND Access

Rule 7b. 'Special considerations apply to any child's file (including child contact record) that is considered to be restricted'

Restricted: Any 'child's file' including its related 'contact records' (child and associated), is of special consideration. Any restricted 'child's file' does not follow the preceding rules e.g. irrespective of Locality membership; but instead has access constrained to a 'whitelist' of specified users, unique to the given child. Those users specified are the only people to have visibility of any aspect of the 'child's file'.

Digital Delivery

CSAS Password Policy

11 December 2019

Accountable Director:	Lawrie McDonald – Programme Director, Digital Delivery Programme
Statement Author:	Bruce Knight – SCRA Digital Governance Lead
Classification	**OFFICIAL**
SIG Review	10 December 2019
Accreditor Review	TBD
SIRO Approval	TBD

Document History and Change Control

Version	Date	Owner	Summary of Changes
0.1	26 Nov 2019	B Knight	First draft
0.2	3 Dec 2019	B Knight	Revised after SIG feedback
0.3	11 Dec 2019	B Knight	Revised after CHS feedback

1 Overview

Passwords are an essential aspect of information security as they are the front line protection to user accounts on SCRA's and CHS's Core System and Applications Solution (CSAS). A poorly chosen password could result in a compromise to personal information held within CSAS. This could have serious consequences for those whose personal details are stored on CSAS.

2 Purpose

The purpose of this policy is to establish a password standard for the Core System and Applications Solution (CSAS), which (where possible), will be enforced through the adoption of technical controls within CSAS. This standard encourage users to select a passphrase or three random words together with at least one capital letter, one number and one special character to create a strong password. By simplifying the construction of the users' passwords, allowing the use of that password for a whole year and allowing users to reset their own passwords, will make it easier for users to manage their password. This standard is to ensure that passwords remain private at all times.

3 Scope

This policy applies to all passwords associated with CSAS in both the SCRA and CHS tenancies. This policy provides specific detail on the construction and storage of passwords for the various account types, whilst defining the management processes for these passwords and the expectations on users.

4 Definitions

Hashing: This is a one-way encryption function where data is mapped to a fixed-length value. Hashing is primarily used for authentication to avoid passwords being kept in clear text.

Master Tennant Account: The master tenant account is the account within the tenancy's Azure Active Directory (AD) with the highest privileges. In a multi-tenancy environment, each Azure AD directory is distinct and separate from other Azure AD directories.

Multifactor Authentication (MFA): Multifactor Authentication is a method of verifying a user's identity by requiring them to present more than one piece of identifying information. MFA creates a layered approach to security by combining two or more independent credentials: what the user knows (password), what the user has (security token) and what the user is (biometric verification). If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target.

Password: A password is a string of characters used to verify the identity of a user during the authentication process. Passwords are associated with a specific username and are designed to be known only to the user to allow that user to gain access to CSAS.

Salting: This is an additional step during hashing, typically seen in association to hashed passwords, that adds an additional value to the end of the password that changes the hash value produced.

SCOTS: The IT infrastructure and networks provided by the Scottish Government that SCRA and CHS use.

Service Accounts: A service account is a special user account that an application or service uses to interact with the operating system. Services use the service accounts to log on and make changes to the operating system or the configuration. Through permissions, you can control the actions that the service can perform.

Two Factor Authentication (2FA): Two-factor authentication is a subset of multi-factor authentication (MFA), where two pieces of information are used to confirm a user's claimed identity. 2FA utilises something they know (their password) with a second factor - something they have, or something they are.

5 Policy

5.1 General Requirements

Most of the accounts on CSAS will use multifactor authentication. SCRA and CHS users working from the secure SCOTS environment will only require their username and password to access CSAS. These users will be registered with multi-factor authentication so that they can reset the password on their account by completing the MFA challenge. By using MFA, SCRA and CHS users will be able to access CSAS through non-SCOTS devices.

Members of the public volunteering to assist with delivering the Children Hearing Service are provided with a volunteer's user account so they can register their details, as part of the recruitment process. If the individual is successful with their application they will be prompted to enrol with two factor authentication so that they can perform their new role. From here they will then be required to use two-factor authentication to get access to CSAS. If they forget their password, they will be required to complete an MFA challenge to reset their password.

5.2 Multi-factor Authentication.

Multi-Factor authentication builds on the standard username and password login approach by adding additional security layers to make it more difficult for an attacker to get access. Adding the need for 'something I have' during login attempts, provides a robust, enhanced user login procedure. During the initial user enrolment with CSAS, the user is prompted to enrol with two factor authentication (2FA) by choosing a secondary authentication method. These include:

1. Email Address
2. Telephone Number (Voice Call)
3. Mobile Telephone Number (Text Message)
4. Microsoft Authenticator App (Code)
5. Microsoft Authenticator App (Notification/Alert)

Users have the opportunity to set their default 2FA method whilst enrolling and have the opportunity to change to any other method after they have logged in.

5.3 Password Properties

Characters Allowed

Letters: A – Z, a - z

Numbers: 0 – 9

Special Characters: @ # $ % ^ & * - _ ! + = [ ] { } | \ : ‘ , . ? / ` ~ " ( ) ; and blank space

Minimum Password Length: Dependant on type of account.

The password must:

i. Not contain a sequential string of numbers e.g. 123456 or characters e.g. abcde

ii. Not contain a well-known keyboard entry, e.g. qwerty

iii. Not contain more than 2 repeating characters, e.g. zzz

iv. Not contain more than two pairs of repeating characters.

v. Not be the same as the User ID.

vi. Not be a blacklisted password

vii. Not be transmitted in the clear or plaintext outside the secure location.

viii. Not be displayed when entered.

Users are encouraged to use:

1. 3 random words of 6 characters or more and separate them with blank character, number or special character, e.g monkey7plastic&Carpet, or
2. select a suitable passphrase adding a number and special character into the passphrase e.g. Like a bridge£4over troubled water

as these are harder to crack.

5.4 Password Management

All passwords are to be hashed and salted before they are stored.

Default passwords must be changed immediately after initial access.

Passwords for the Master Tenant Account and Service Accounts must be stored in a KeyVault or other appropriately secure password repository. Privileged Users (i.e. Global Admin and System Admin) and Standard Users are expected to manage the security and privacy of their passwords in accordance with this Policy.

As part of the CSAS Leavers and Dormant Accounts process, accounts which are marked as dormant or identified as part of the Leavers process must be deleted or disabled. For example, when a user retires, quits, is reassigned/seconded, dismissed, etc.

5.5 Password Protection Standards

SCRA and CHS staff must not use their SCOTS User ID as their CSAS password.

CSAS users must set up a unique password for CSAS and not use it for accessing any sites for personal use.

CSAS users must not share their CSAS password with anyone. All passwords are private and confidential and are to be treated as such.

Here is a list of "do not's"

- Do not reveal or discuss your password verbally or in writing to anyone
- Do not hint at the format of your password (e.g., "my family name")
- Do not reveal your password on questionnaires or security forms
- Do not share your password
- Do not store passwords in ANY computer system that is unencrypted.

5.6 Password Standards

5.6.1 Azure Master Tenant Account

Minimum Password Length	30
Password structure	Randomly generated
Password Expiry	When changing IT Support Contractor
Lockout Attempts	Never
Minimum Number of Upper Case	2
Minimum Number of Lower Case	2
Minimum Number of Numbers	2
Minimum Number of Special Characters	2
Multifactor Authentication Required	Yes

5.6.2 Service Accounts

Minimum Password Length	24
Password structure	Randomly generated
Password Expiry	Never
Lockout Attempts	Never
Password Rotation	Every 6 months
Minimum Number of Upper Case	2
Minimum Number of Lower Case	2
Minimum Number of Numbers	2
Minimum Number of Special Characters	2
Multifactor Authentication Required	Preferred

5.6.3 Privileged User Accounts

Minimum Password Length	24
Password structure	Randomly generated
Password Expiry	Every 12 months
Lockout Attempts	Locked out after 5 attempts
Minimum Number of Upper Case	1
Minimum Number of Lower Case	1
Minimum Number of Numbers	1
Minimum Number of Special Characters	1
Minimum Password Re-Use	After 12 uses
Multifactor Authentication Required	Yes

5.6.4 User Accounts

Minimum Password Length	20
Password Expiry	Every 12 months
Password Notification	14 days before expiry date
Lockout Attempts	Locked out after 5 attempts
Lockout Reset	After 10 minutes
Minimum Number of Upper Case	1
Minimum Number of Lower Case	1
Minimum Number of Numbers	1
Minimum Number of Special Characters	1
Minimum Password Re-Use	After 12 uses
Resetting Forgotten password	Last password can be reused
Multifactor Authentication Required	Preferred

6 Penalties

Any SCRA or CHS employee found to have breached this policy could face disciplinary action in accordance with their own organisation's disciplinary policy and procedures. CHS Volunteers who breach this policy will face action in accordance with CHS policies.

Advocacy Communication information for SCRA EMT Decision Making
(reviewed and approved prior to EMT consideration by SG Advocacy Team).

EMT are asked to decide if we can:

a) add a sentence to our letters (wording to be agreed with Scottish Gov Advocacy Team)

"Advocacy for Children's Hearings is available across Scotland to children and young people to understand what is happening and participate by giving their views and wishes within their Children's Hearing. If this would be a useful support for you / your child or if you would like to learn more about advocacy you should contact the Children's Hearings Advocacy Service in your area. Their details are online at…….and your social worker will also have the details."

and a Web link with every Hearing notification

b) send a revised leaflet

POSSIBLE REVISED LEAFLET INFO

Amend the All About Children's Hearings Leaflet (*suggested amendment only – Comms team and OHOV have already planned to look at the leaflet after Christmas*):

the *Why do I have to go to a Hearing?* section – first sentence There are lots of reasons for a Children's Hearing. You should know why you are coming to the hearing and if you don't then you should ask.

the *Where will it be?* section - last sentence – Then you will go into the Hearing room and meet the Children's Panel members who will make the decision in your Hearing.

the *Who will be there?* Section – last sentence – Your social worker will be there and other people may also be there like your teacher.

The *You will get asked some questions?* Section – *How are you? Do you know why you are here? What do you want to happen? What do you think about things?*[1] The Panel Members may ask you some questions to make sure you get the right help.

the *Having Your Say* section – The Hearing is all about you and you are the most important person there. The Panel members in the Hearing want to hear from you and want to know what you would like to happen. If you would like to be supported by someone to tell the Hearing what you think then that can happen. You could give the hearing an All About Me form, or write something else or draw a picture or make a presentation. The Children's Hearing wants to hear what you have to say.

the *Your rights* section – You might want to speak with someone before the Hearing, to make sure you understand what the Hearing is about and to make sure the

[1] Check with CHS Training re: asking questions of children. What examples are in the training?

Hearing will hear what you want to say. You can bring someone to help and support you if you want. You might want to ask the Hearing some questions. It may help you if a specially trained person, like an advocacy worker, a legal representative or a children's rights officer is also involved to help you tell the Hearing what you think, to help you ask questions and to help you understand what is happening.

The *What might happen?* section – The Panel Members in the Children's Hearing will read all the information they are sent before the Hearing and will listen to everyone during the Hearing. They will make the best decision for you. If you are in the Hearing they will tell you what is going to happen and why. If you would like someone to explain what happened after the Hearing then you should say so.

c) POSSIBLE NEW LEAFLET To be sent with Reporter decision – arrange Hearing letter and ALL Hearing notifications AND / OR to be online as information on SCRA / CHS / CHIP websites AND / OR to be used by SW and / or education in discussion with children as part of preparation for their Children's Hearing.

Children's Advocacy in Children's Hearing's

The Scottish Government has set up provision for Children's Hearing Advocacy.

Advocacy workers support children and young people to understand what is happening and help them to participate by giving their view in the Children's Hearing.

Advocacy workers champion children and young people by listening to them to understand their life and what matters to them and by helping them to understand and exercise their rights and opinions in the Hearings.

Advocacy workers are working in all 32 Local Authorities in Scotland and will be available to help you, if you want.

Your social worker will speak with you to make sure you understand what is happening, so that you know why there is going to be a Children's Hearing and you know what the Children's Hearing are going to talk about. Your social worker will also speak with you about how you can tell the Children's Hearing what you think.

Your social worker will let you know that, if you want, you can speak with an Advocacy worker. If you think this would help you then your social worker will pass your details on and the Advocacy worker will contact you to let you know about how they can help.

The Advocacy worker will speak to you before the Children's Hearing, will support you during the Hearing and will explain what happened in the Hearing after it has finished. The Advocacy worker will also help you understand what will happen next and what you can do about things.

If you are supported by an Advocacy worker for the Children's Hearing then this worker will also be available to support you in other meetings about your Hearing. If

you are already supported by an Advocacy worker for another reason then this worker may also be able to provide you with support in the Children's Hearing.

and a Web link with every Hearing notification

d) develop a script w SW Scotland so Reporters discuss w SW and SW discuss w families and add in their reports.

- Localities could develop their MoU with LA's to include the expectation that the offer of advocacy is covered in assessment?

e) add a section to the email sent to SW to confirm the date and time of a CH and direct all localities to use this (add as a signature for all Reporters / Ass Reps):

OFFICIAL-SENSITIVE PERSONAL

We have received your request for a hearing alongside the Social Work Report for :CHILDS NAME

To keep in line with our timescales I have pencilled the hearing into our diary for :DATE & TIME.

Please confirm the suitability of this date by return email and I can go ahead and schedule.

If this date is not suitable, please contact me on the number below to discuss an alternative arrangement. If I don't hear from you we will notify the hearing at the date and time detailed above in 5 working days

DATE & TIME for PHP.

Address Checks

Can you please confirm if RP's address is: XXX

Can you please confirm childs's address is : XXXXX

Invitees

I am inviting : XXXX, XXX, XXXX
and will request a full report from the above named agencies

Please mark as appropriate

Information about the availability of Advocacy services will be sent to CHILD'S NAME. It would be helpful if you could speak about this with them.

Are there any other special circumstances surrounding this hearing that I need to be aware of ?

Health & Safety
Separate waiting rooms
Police attendance
Interpreter / Sign Language

Many thanks

e) In collaboration with CHS we develop a poster / a cartoon for young children / a film for older children and a film for panel members (which would also be of benefit to Reporters) about advocacy, which can be hosted online. SG are still to decide if a discreet website for Children's Hearing Advocacy provision should be developed – on reflection it probably SHOULD – as it means that there is a single place to direct people to for the national information and signals the independence from decision makers eg. the local authority/social worker, SCRA and CHS. There is limited money available for publicity work. SG will also be updating the key principles of the service to ensure alignment with the SIAA refreshed practice of children's advocacy and issue the final practice model – but these docs would be the basis for anything that is developed.